Foreword

Establishing, evaluating and monitoring the effectiveness of internal controls over financial information is an important issue which is the responsibility of all public sector entities; and entities’ approaches to these matters are considered by the Australian National Audit Office (ANAO) in determining our audit coverage of entities’ financial statements.

The use of technology and IT systems is increasingly embedded into business processes to initiate, authorise, process and manage financial transactions. As a result, weaknesses in the design or operation of technology have the potential to not only compromise the integrity and accuracy of financial information, but may impede the efficiency of an entity to achieve its objectives.

SAP continues to be a prominent system used by many Australian Government entities for planning, managing and reporting of business and financial information. In addition to the traditional uses of reporting of financial transactions, material procurement and asset management; SAP now increasingly supports the business functions of human resource management, services management, and business process management.

This SAP ECC 6.0 Security and Control Better Practice Guide updates and consolidates the previous two SAP Handbooks released by the ANAO. Coverage of the guide has been extended to provide a fuller appreciation and understanding of functionality changes to SAP and to increase awareness of current practices for efficient and effective management of SAP. It is anticipated that this guide will be useful for a range of staff, including system managers, chief financial officers, chief information officers and system users.

It is important for entities to individually assess the importance and relevance of the implementation of practices described in this guide. Choosing which controls to implement and use, and the extent of their use, also depends on how cost-effective, appropriate and relevant a particular practice is to an entity.

The ANAO thanks contributors to this guide, including Protiviti Australia and SAP Australia.

Ian McPhee
Auditor-General

June 2009
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>i</td>
</tr>
<tr>
<td><strong>Chapter 1 – Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>Purpose of this guide</td>
<td>3</td>
</tr>
<tr>
<td>Structure</td>
<td>3</td>
</tr>
<tr>
<td>Why consider controls?</td>
<td>4</td>
</tr>
<tr>
<td>Previous guides and this guide</td>
<td>4</td>
</tr>
<tr>
<td>How to read this guide</td>
<td>5</td>
</tr>
<tr>
<td><strong>Chapter 2 – Procurement and payables</strong></td>
<td>9</td>
</tr>
<tr>
<td>2.1 Procurement and purchasing activities</td>
<td>13</td>
</tr>
<tr>
<td>2.2 Supplier Relationship Management (SRM)</td>
<td>22</td>
</tr>
<tr>
<td>2.3 Vendor Master File</td>
<td>29</td>
</tr>
<tr>
<td>2.4 Material Master File</td>
<td>36</td>
</tr>
<tr>
<td>2.5 Receipt of goods or services</td>
<td>40</td>
</tr>
<tr>
<td>2.6 Invoice Processing</td>
<td>46</td>
</tr>
<tr>
<td>2.7 Payment Processing</td>
<td>55</td>
</tr>
<tr>
<td><strong>Chapter 3 – General Ledger</strong></td>
<td>61</td>
</tr>
<tr>
<td>3.1 General Ledger Master Maintenance</td>
<td>64</td>
</tr>
<tr>
<td>3.2 General Ledger Postings / Reconciliation</td>
<td>71</td>
</tr>
<tr>
<td>3.3 New General Ledger</td>
<td>78</td>
</tr>
<tr>
<td><strong>Chapter 4 – Human Resources</strong></td>
<td>87</td>
</tr>
<tr>
<td>4.1 Personnel Management</td>
<td>90</td>
</tr>
<tr>
<td>4.2 Personal Time Management</td>
<td>98</td>
</tr>
<tr>
<td>4.3 Payroll Accounting</td>
<td>102</td>
</tr>
<tr>
<td>4.4 Employee Self Service</td>
<td>110</td>
</tr>
<tr>
<td>4.5 Managers Desktop</td>
<td>114</td>
</tr>
</tbody>
</table>
Chapter 5 – Basis

5.1 Transport Management System

5.2 Security

5.3 Table and Program Maintenance

5.4 Basis System Administration

5.5 Mass Maintenance

5.6 NetWeaver Security

5.7 Central User Administration

5.8 Backup and Recovery

5.9 Portal Security (SAP Enterprise Portal)

Chapter 6 – Controlling

Overview

Functional overview

Commonly identified control weaknesses

Significant risks

Risks and controls

Security considerations

Optimising the SAP control environment

Chapter 7 – Project System

Functional overview

Commonly identified control weaknesses

Significant risks

Risks and controls

Security considerations

Optimising the SAP control environment

Chapter 8 – Asset Accounting

8.1 Asset Master Maintenance

8.2 Asset Transaction Postings
### Appendices

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix 1 – Terminology and definitions</td>
<td>247</td>
</tr>
<tr>
<td>Appendix 2 – Upgrading to ECC</td>
<td>265</td>
</tr>
<tr>
<td>Appendix 3 – SAP and segregation of duties risks</td>
<td>267</td>
</tr>
</tbody>
</table>

### Feature articles

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 3 – Feature article</td>
<td>81</td>
</tr>
<tr>
<td>Chapter 5 – Feature article</td>
<td>173</td>
</tr>
<tr>
<td>Chapter 7 – Feature article</td>
<td>221</td>
</tr>
</tbody>
</table>

### Case studies

<table>
<thead>
<tr>
<th>Case Study</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up release strategy approval limits</td>
<td>16</td>
</tr>
<tr>
<td>Eliminating vendor maintenance, segregation of duties concerns using dual control for sensitive fields</td>
<td>31</td>
</tr>
<tr>
<td>One-time vendor (OTV) payments</td>
<td>33</td>
</tr>
<tr>
<td>Duplicate invoice check</td>
<td>48</td>
</tr>
<tr>
<td>OCR invoice scanning</td>
<td>53</td>
</tr>
<tr>
<td>Periodic assessment for employees who are paid as vendors</td>
<td>92</td>
</tr>
<tr>
<td>Cross-Talk in SAP Security</td>
<td>129</td>
</tr>
<tr>
<td>Monitoring for Cross-Talk issues which result in problems with access across organisational areas</td>
<td>130</td>
</tr>
<tr>
<td>Single sign-on for SAP systems</td>
<td>135</td>
</tr>
<tr>
<td>User versus position based security</td>
<td>145</td>
</tr>
<tr>
<td>Logging changes to critical tables</td>
<td>147</td>
</tr>
<tr>
<td>Implementing preventative controls to monitor segregation of duties risks</td>
<td>183</td>
</tr>
<tr>
<td>Improving the accuracy of depreciation charges using Asset Class Useful Life configuration controls</td>
<td>239</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

Purpose of this guide  3
Structure          3
Why consider controls?  4
Previous guides and this guide  4
How to read this guide  5
Purpose of this guide

This guide is intended to assist Australian Government entities to strengthen security and controls within SAP. It will be a useful guide to assist entities that are looking to:

- identify and assess business impacts that may arise as a result of control weaknesses;
- increase awareness of risks to security and control within SAP;
- strengthen system security controls and ensure that user access to key transaction codes and authorisation objects are appropriately restricted and segregated; and
- implement better practice procedures to improve delivery of financial processes.

Structure

Each SAP module has been divided into the major processes or functions that are performed within that module. The figure below depicts the structure of the better practice guide.
Why consider controls?

SAP continues to be a prominent financial system used by many Australian Government entities. Approximately 70 per cent of large government entities currently use SAP as their financial management system. These entities account for approximately 80 per cent of government revenues and over 70 per cent of total expenses.

Increasingly, the financial reporting process for Australian Government entities is driven by information systems. The use of technology and IT systems is embedded into business processes to initiate, authorise, process and manage financial transactions.

Today’s SAP financial management systems, have complex interfaces with internal business systems, interface with numerous IT processing or reporting systems and receive or transfer financial information concerning government payments or grant payments. Government entities are also increasingly implementing ‘shared services’, whereby one government entity has responsibility for the processing and/or system management of financial transactions on behalf of another government reporting entity. Financial management systems used by entities within the general government sector may have as few as 10 personnel or as many as 5,000 personnel accessing an entity’s SAP system. In order to encourage flexible working practices, IT services are introducing and expanding functionality that allow users access to the financial management system via web-portals, ‘remote access’ and virtual networks, and increasingly the use of synchronised sign-on or single sign-on (SSO) is being adopted by entities to facilitate identity management.

As a result, IT systems such as SAP are not only inextricably linked to the overall financial reporting process but form the foundation of an effective system of internal control for financial reporting.

Previous guides and this guide

The original Security and Control for SAP ERP Handbook, developed in 1998, was produced to provide better practice security and control guidelines when implementing and running SAP Version 3.1H. In 2004, the ANAO published an update guide, the Security and Control for SAP ERP Handbook Update, based on SAP ERP Release 4.6C. It outlined significant functional enhancements with relevant security and control considerations to be read in conjunction with the original handbook.

Since the release of the update guide, the SAP application has undergone a significant number of functionality changes. In addition, government and business practices and requirements for managing and reporting financial information have changed.

This guide is both an update and consolidation of the previous two guides. Content has been expanded to address current SAP functionality and considers current risks facing system and business managers.

---

Areas covered by this guide

This guide covers those modules of SAP that are most likely to be implemented by public sector entities. They are: Procurement and Payables; General Ledger; Human Resources; Basis; Controlling; Project System; and Asset Accounting. In addition, the guide contains several supplementary feature articles on emerging topic areas, including: implementing effective access control to the SAP Governance, Risk and Compliance module; and include issues for consideration when implementing financial shared services or grants management. A detailed glossary of terms is provided in the Appendix, as are key areas to consider when upgrading a SAP installation to ECC 6.

Areas not covered by this guide

There are other modules in SAP that are not used commonly by public sector entities and, therefore, are not covered by this guide. They include: Sales and Distribution; Treasury; Investment Management; Real Estate Management; Customer Service; Training and Event Management; Production Planning; Quality Management; Plant Maintenance; and Office Communications.

How to read this guide

Each SAP module has been divided into the major processes or functions that are performed within that module. Each function is introduced with a brief narrative (functional overview) followed by several sections as described in the following paragraphs.

Commonly identified control weaknesses

The guide details areas specific to the business process or SAP function that are vulnerable to control weaknesses if not implemented or maintained. Descriptions of why these areas are vulnerable and what can be done to address them are also presented.

Risks and controls

The guide highlights key risks specific to the function and details the controls that are required to mitigate these risks. Risks and controls are identified in this guide using an ‘R’ for Risk and a ‘C’ for Controls, and are each given a unique number for easy identification. The maintenance of security in SAP, and therefore the existence of controls to mitigate risks, is not desirable – it is critical. Therefore, entities must have controls in place to mitigate these risks. The controls need not be exactly the same as the ones described in this guide – an entity may have ‘compensating controls’ to mitigate these risks (controls different to the ones in this guide that help mitigate risks), or a combination.

Not every risk listed will be applicable to every entity using SAP. This is variable from entity to entity depending on factors such as the nature of the business they conduct, the size of the entity, the resourcing of the entity, its level of acceptable risk, and the modules of SAP it has decided to implement.
Risk rating key

There are numerous methods for classifying or identifying risks. The following is the approach that has been adopted by the ANAO for the classification of risks in this guide.

**High**
- Poses a significant financial reporting risk
- Likely to involve complex system configuration requirements
- Likely to involve high resource (personnel and/or infrastructure resource) commitment

**Medium**
- Poses a moderate financial reporting risk
- Likely to involve less complex system configuration requirements
- Likely to involve moderate resource (personnel and/or infrastructure resource) commitment

**Segregation of duties risks**
- Poses an increased risk of fraud
- The risk may be mitigated through restricting access to users

Low risk controls are not described in this guide. Rather, the guide has added detail for entities to consider in sections in each chapter titled ‘Optimising the SAP control environment’ and ‘Implementation considerations for ECC’. Entities should review the relevance of the risks presented in this guide and the risk classification according to the entity’s operations and circumstances.

**Optimising SAP controls**
- Controls that, if implemented, will improve the efficiency with which an entity manages SAP, or improve the operating effectiveness of existing controls.

**Implementation considerations**
- Controls or activities to consider when implementing system upgrades. Failure to consider these issues when implementing ECC or upgrading may reduce the effectiveness of other system controls.

Optimising SAP controls

This section in each chapter describes better practice procedures that, if implemented, are likely to improve the efficiency with which an entity manages SAP, or improve the operating effectiveness of existing controls.
Implementation considerations

Implementation considerations refer to controls or activities that entities should consider undertaking when upgrading or implementing certain controls that may be complex to either implement or to define user requirements.

Risk checklist

The following checklist may be of use to entities in determining the relevance of risks or to prioritise controls an entity may implement to improve the effectiveness of the controls environment.

- Is the risk being assessed related to a material balance? [Yes/No]
- Does the entity process a high volume of similar transactions? [Yes/No]
- Do system users apply a high level of judgement in initiating or processing financial information? [Yes/No]
- Is there a high level of manual intervention in processing of financial information? [Yes/No]
- Does the entity place a high level of reliance on other entities to process financial transactions, or to manage the SAP system? [Yes/No]

A ‘YES’ response to three or more of the above questions indicates a HIGH risk and increased probability of being a significant reporting risk.

Application controls

Application controls refer to several types of controls. The term refers to controls by users, data management and processing controls. This guide provides suggested configuration and manual controls.

Critical controls are marked with a ‘!’ to indicate a control that, if not implemented, increases the likelihood that other dependent controls will not be satisfied.

Configuration controls are detailed in this guide. These usually involve changing or modifying a setting within the SAP system in order to implement a control.

Manual controls refer to a management or monitoring practice that may be performed by an entity. Often, this control refers to a report that may be provided from a SAP system that may be used to review or detect irregularities.

Manual controls are often described or referred to as ‘detective controls’ as they provide information that may be reviewed or analysed in order to detect irregularities. A number of risks in this guide recommend implementation of manual controls as they facilitate validation or ‘checks’ to confirm that a control activity has been authorised.
In order for manual controls to operate effectively, careful consideration should be given to the design of the report content and the timing of review activities to ensure that information reviewed is sufficient and suitable for the intended purpose. Manual or process controls implemented independently of corresponding configuration controls, or implemented ‘in lieu’ of a configuration control, will rarely provide an effective safeguard to prevent significant risks, however, properly designed they may be effective to detect and report control weaknesses.

**Security considerations**

Effective security controls are essential to ensure the accuracy and reliability of data maintained by the IT application and the operational reliability and performance of the system.

The *Protective Security Manual* requires Australian Government entities to protect information resources, including ICT systems, from compromise and misuse.3 Entities should also refer to the *Australian Government ICT Security Manual* (ISM)4 which outlines a combination of physical, personnel, information, IT and communications measures to assist entities to implement IT security controls that satisfy the minimum standards required to protect information stored or transmitted via electronic means.5

SAP security controls are inherently complex and require considerable knowledge and skill to implement. This guide highlights significant security risks and recommendations for optimising security and access controls for SAP. Chapter 5 details risks for management of Basis and general security considerations.

**Transaction codes and authorisation objects**

The foundation of SAP security relies upon authorisation objects and transaction codes which establish user access rights. This guide highlights key transaction codes and authorisation objects specific to SAP components that must be restricted to appropriate staff in order to mitigate access risks and segregation of duties risks.

**Segregation of duties**

In SAP terms, a segregation of duties risk is an object that associates two or more conflicting functions. A function is a task that an employee performs to accomplish a specific portion of his/her job responsibilities. Appendix 3 provides further information on principles for segregating SAP functions.

**Link to other SAP components or better practice**

Throughout this guide, this symbol ☐ is used to indicate where a control or feature references other sections in the document, or references other ANAO Better Practice Guides. ANAO Better Practice Guides may be accessed electronically at the ANAO’s website: www.anao.gov.au.

---

Chapter 2

Procurement and payables

2.1 Procurement and purchasing activities 13
2.2 Supplier Relationship Management (SRM) 22
2.3 Vendor Master File 29
2.4 Material Master File 36
2.5 Receipt of goods or services 40
2.6 Invoice Processing 46
2.7 Payment Processing 55
IMPORTANT UPDATE
Procurement cycle overview

Procurement cycle description

1 – Purchase requisitioning

Typically, a purchase requisition is raised for all goods/services that an entity procures. Requisitions may be raised with reference to a contract or outline agreement which specifies a certain volume that should be purchased from a particular vendor. The ability to approve/release purchase requisitions should be controlled via release procedures in the SAP system to ensure that only employees with the appropriate authority can authorise a purchasing transaction.

2 – Vendor selection

The system can also suggest an appropriate vendor for the products being procured via source determination (a vendor may be selected from a source list). Where appropriate, the system should enforce a vendor evaluation process via ‘request for quotation’ functionality.
### 3 – Purchase order processing

Purchase orders can then be created based on the requisitions and any related quotations. Purchase orders should be required to reference an approved purchase requisition. Any changes to the purchase requisition or purchase order should be subject to the appropriate approval procedures. Appropriate reports should be used to monitor long outstanding purchase orders.

### 4 – Goods receipt

A goods receipt, or the acceptance and entry of products, should be performed for each purchase order. The goods receipt should be processed with reference to the corresponding purchase order. The acceptance and entry of goods/services should be separated to ensure the appropriate authorisation of services accepted for payment.

### 5 – Invoice processing

Invoices are processed with reference to the appropriate purchase order and goods receipt via the invoice verification process. Any invoices that do not match the purchase order and goods receipt details within defined tolerances are automatically blocked for payment.

Invoices that do not have a valid purchase order in the system (i.e. utility payments) should be processed separately via the Financial Accounting Accounts Payable module. These invoices are not subject to requisition approvals. However, non-purchase order invoices should be subjected to payment release procedures used in conjunction with SAP’s ‘park and post’ and Workflow functionalities to ensure that all invoices beyond a certain amount are authorised in accordance with approved delegation levels.

### 6 – Payment processing

Payments and the claiming of prompt payment discounts are driven by the payment terms, which should be entered in the vendor master record and should not be changed in the purchase order or invoice. Payment runs should be performed on a regular basis and all payment reports, including payment exceptions (i.e. blocked invoices), should be reviewed to ensure all payments are reasonable. Manual cheques should not be used, as the payment program can be run as frequently as required to process payments. This ensures an adequate level of control over payments and reduces the risk of unauthorised payments.
2.1 Procurement and purchasing activities

Functional overview

Purchase requisitions can be raised manually and should be subject to an electronic approval procedure. Requisitions may be released to a request for quote, requesting vendors to provide a quotation. A purchase order is created either from the purchase requisition automatically or may be created manually. The system can suggest possible sources of supply based on past orders (info records), contracts, or outline agreements. The purchase order is then raised and output to the vendor.
Procurement process components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Materials requirements planning (MRP)</td>
<td>A planning process used prior to production of goods or projects to determine the exact materials and quantities necessary for completion.</td>
</tr>
<tr>
<td>Material Master File</td>
<td>A master data record created for every raw or finished material utilised by an entity.</td>
</tr>
<tr>
<td>Purchase requisition</td>
<td>A request to acquire a defined quantity of specified products.</td>
</tr>
<tr>
<td>Purchase order</td>
<td>An order placed with a vendor for specified quantities of products at a particular price.</td>
</tr>
<tr>
<td>Blanket purchase order</td>
<td>A purchase order created with a value limit and a validity period instead of a delivery date. A blanket purchase order allows a user to procure various products from vendors in cases where the creation and processing of individual purchase orders is not deemed economical. Blanket purchase orders would generally be utilised for low value, high use items for which this process is deemed appropriate.</td>
</tr>
<tr>
<td>Vendor Master File</td>
<td>A master data record containing name, address, payment details, etc. This is created for every entity from whom an entity purchases products.</td>
</tr>
</tbody>
</table>

Commonly identified control weaknesses

The following control weaknesses typically occur in the procurement and purchasing process:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to properly design release strategies</td>
<td>Configuring release strategies for proper approval routing is complex; often, strategies do not cover all purchasing types or scenarios. Release indicators should also be set so that any changes made after approvals are made will be subjected to a new release strategy and possibly re-approval.</td>
</tr>
<tr>
<td>Purchase orders are created without referencing approved purchase requisitions</td>
<td>A configuration parameter setting needs to be defined to prevent purchase orders from being directly created (without reference). Without this setting in place, release strategies will be compromised.</td>
</tr>
<tr>
<td>Failure to prevent users from overriding tolerances, terms, and indicators</td>
<td>It is possible for users to manually change over delivery tolerances, payment terms and goods receipt indicators when completing purchasing documents. These parameters need to be controlled so that system configured tolerances and vendor specific terms cannot be altered.</td>
</tr>
<tr>
<td>Purchase price tolerances not set</td>
<td>SAP can be configured to give the user a warning message when the purchase order is saved if there is a difference between the price entered on the purchase order and the price stored on the system; however, this does not restrict the order from further processing. Therefore, purchase price tolerances need to be appropriately defined to prevent any harmful errors or fraudulent activity.</td>
</tr>
</tbody>
</table>
Significant risks

High
- Unapproved purchase requisitions/orders are created
- Changes are made to approved requisitions or orders
- Purchase orders do not reference purchase requisitions

Medium
- Approved blanket purchase order values are exceeded
- Non-strategic vendors are used for purchasing
- Invoice and goods receipt settings are changed in purchase order creation

Segregation of duties risks
- Purchasing Document Creator and Purchasing Document Approver
- Purchasing Approver and Goods Receipt

Risks and controls

R200: Unapproved purchase requisitions/orders are created

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Unauthorised purchase orders or requisitions may be processed which do not comply with an entity’s delegations of authority. This can result in the processing of unauthorised or fraudulent expenditure.</td>
</tr>
</tbody>
</table>

Controls

Configuration controls

Release strategies are the key control for the authorisations of purchase requisitions and/or purchase orders. Release strategies are defined for a determined monetary amount, which allows an entity to set its delegation of authorities within the SAP system. Strategies are optimally designed with classification or, in correlation with position security and the SAP HR module, allowing for line item approvals. Strategies designed without classification only allow for approvals of an entire purchasing document.

Release strategies should be defined for both purchase requisitions and purchase orders. (C229)
**Setting up release strategy approval limits**

When implementing release strategies, entities typically decide on whether to implement strategies on purchase requisitions or purchase orders or on both.

An entity was using both purchase requisitions and purchase orders, but decided to implement release strategies only on requisitions. Their rationale was that purchase orders were created by the purchasing department who required autonomy to improve the efficiency of purchasing activities.

The entity’s Internal Audit group, during a purchasing review, identified that a number of purchases were processed without a purchase requisition which increases the risk of inappropriate purchases being made. The entity subsequently decided to implement release strategies on both requisitions and orders.

Source: Protiviti Australia

<table>
<thead>
<tr>
<th>R201: Changes are made to approved requisitions or orders</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk rating</strong>: HIGH</td>
</tr>
<tr>
<td><strong>Risk description</strong>: The effectiveness of release strategies for purchasing approvals depends heavily on whether approved purchases can be subsequently changed without further approval. If so, then this can lead to unauthorised or fraudulent expenditure.</td>
</tr>
<tr>
<td><strong>Controls</strong>: Functional authorisations can be used to control a number of risk areas, including: (1) ability to change approved requisitions, (2) ability to display prices, and (3) ability to create a purchase order without references to a purchase requisition. By default, users have the ability to perform all three functions. Therefore, the functional authorisations should be allocated to required users as parameter values in their user master record (transaction SU01).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R202: Purchase orders do not reference purchase requisitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk rating</strong>: HIGH</td>
</tr>
<tr>
<td><strong>Risk description</strong>: Purchase orders are placed with vendors for materials, quantities, and prices that have not been approved by the proper authoriser. This could lead to an entity suffering undue financial burden.</td>
</tr>
<tr>
<td><strong>Controls</strong>: Mandatory purchase requisition reference Some entities require that all purchase orders reference a valid purchase requisition. This is extremely important in situations a where purchase order release approval strategy has not been implemented. The requisition field should be made mandatory during purchase order creation to force users to reference a valid purchase requisition.</td>
</tr>
</tbody>
</table>

Source: Protiviti Australia
### R203: Approved blanket purchase order values are exceeded

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Key risks include:</td>
</tr>
<tr>
<td></td>
<td>If blanket purchase orders are being used, invoices which may exceed the total of the blanket purchase order may be processed.</td>
</tr>
<tr>
<td></td>
<td>No goods receipt or entry and acceptance of services is required with blanket purchase orders; invoices are posted directly with reference to the order. This may result in the bypassing of purchasing controls.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>Tolerance codes</strong></td>
</tr>
<tr>
<td></td>
<td>Tolerance code “LA” should be set to check the sum of value invoiced so far against the value limit of the purchase order. (C468)</td>
</tr>
<tr>
<td></td>
<td>Tolerance code “LD” determines whether the posting date of the invoice is within the tolerance of the blanket purchase order’s valid time. (C468)</td>
</tr>
</tbody>
</table>

### R204: Non-strategic vendors are used for purchasing

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Source determination provides an opportunity to optimise the number of suppliers used to purchase certain products. Without source determination, an entity may be paying more for the purchase of products and services and/or receiving reduced levels of service.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>Source determination</strong> is a useful control to ensure that vendors which provide the best service and price for a particular product are selected throughout an entity. Source determination determines the source of supply for individual material items. (C230) There are two options when configuring:</td>
</tr>
<tr>
<td></td>
<td>• Define a regular vendor: if several vendors are determined, the vendor flagged as the regular vendor will be suggested.</td>
</tr>
<tr>
<td></td>
<td>• Source lists: A source of supply should be entered in the source list before a purchase order issued to a vendor can be processed.</td>
</tr>
<tr>
<td>Risk rating</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Risk description</td>
<td>Failure to configure the invoice and goods receipt indicators can impact on the integrity of the three way match process and result in the over receipting of payment of purchase order items.</td>
</tr>
<tr>
<td>Controls</td>
<td><strong>Configuration controls</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Item category settings</strong> control the method of processing purchasing transactions in SAP. An example is whether a goods receipt is required; or whether an invoice receipt and/or material number is required for the transaction. (C1024)</td>
</tr>
<tr>
<td></td>
<td><strong>Setting GR indicator binding parameter to on</strong></td>
</tr>
<tr>
<td></td>
<td>The ‘GR indicator binding’ parameter should be set to ‘on’ to ensure that matching of invoices to goods receipt cannot be bypassed. If this is not set, it could allow an invoice to be processed for goods/services that have not actually been received. (C1025)</td>
</tr>
</tbody>
</table>
## Security considerations

Standard purchasing transactions and security objects that should be restricted to appropriate purchasing staff.

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transactions</strong></td>
<td></td>
</tr>
<tr>
<td>ME51, ME51N</td>
<td>Create Purchase Requisition</td>
</tr>
<tr>
<td>ME54</td>
<td>Release Purchase Requisition</td>
</tr>
<tr>
<td>ME21, ME21N</td>
<td>Create Purchase Order</td>
</tr>
<tr>
<td>MEPO</td>
<td>Create/Change Purchase Order</td>
</tr>
<tr>
<td>MEMASSPO</td>
<td>Mass Change of Purchase Orders</td>
</tr>
<tr>
<td>ME28</td>
<td>Release Purchase Order</td>
</tr>
<tr>
<td>MB01, MB0A</td>
<td>Post Goods Receipt for Purchase Order</td>
</tr>
<tr>
<td>MB1C</td>
<td>Other Goods Receipts</td>
</tr>
<tr>
<td><strong>Authorisation Objects</strong></td>
<td></td>
</tr>
<tr>
<td>M_BEST_WRK, M_BANF_WRK</td>
<td>Purchase Order creation for each plant location.</td>
</tr>
<tr>
<td>M_BEST_BSA</td>
<td>Purchase Order creation for each Purchasing Document Type</td>
</tr>
<tr>
<td>M_BANF_BSA</td>
<td>Purchase Requisition creation for each Purchasing Document Type</td>
</tr>
<tr>
<td>M_BANF_FRG</td>
<td>Release Code in Purchase Requisition</td>
</tr>
<tr>
<td>M_EINK_FRG</td>
<td>Release Code and Group (Purchasing)</td>
</tr>
<tr>
<td><strong>Entity Values</strong></td>
<td></td>
</tr>
<tr>
<td>EKORG</td>
<td>Purchasing Entity</td>
</tr>
<tr>
<td>EKGRP</td>
<td>Purchasing Group</td>
</tr>
<tr>
<td>WERKS</td>
<td>Plant</td>
</tr>
<tr>
<td>BSART</td>
<td>Purchasing Document Type</td>
</tr>
</tbody>
</table>

### Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchasing Document Creator</td>
<td>Purchasing Document Approver</td>
<td>Should not be allowed to create and release the same purchasing document – could result in the approval of unauthorised and/or inappropriate purchasing documents.</td>
</tr>
<tr>
<td>Purchasing Approver</td>
<td>Goods Receipt</td>
<td>Could approve a purchase and then process a fictitious goods receipt or misappropriate the goods.</td>
</tr>
</tbody>
</table>
## Optimising the SAP control environment

### Optimising SAP controls

- Required fields for entry
- Vendor/material master auto-populated fields
- Restricted fields from user input
- Incomplete purchase orders
- Follow up of outstanding purchase orders
- Material tolerance
- Electronic authorisations for purchase requisitions
- Electronic authorisations for purchase orders
- Optional automatic generation of purchase orders

The following items should be considered to improve the efficiency and control of the purchasing process:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required fields for entry</strong></td>
<td>The ‘field status’ for purchasing documents (purchase requisitions, purchase orders, contracts, source lists, info records) should be set to ensure that all critical fields necessary to complete the document are set to ‘required entry’. Fields which are not mandatory should be set to ‘optional entry’.</td>
</tr>
</tbody>
</table>
| **Vendor/material master auto populated fields** | Some fields for purchasing documents are set as ‘required entry’ by SAP and cannot be changed (i.e. document type, purchase order number, material number, price, delivery date). Additional fields which should be defaulted from the vendor/material master record include:  
  - Item category  
  - Payment terms (set as ‘display only’)  
  - Currency (for multiple currency companies)  
  - Account assignment  
  - Under and over-delivery tolerances (set as ‘display only’)  
  - GR control indicators (set as ‘display only’) |
| **Restricted fields from user input** | It is also possible to enter sensitive parameters/information within the purchase order transaction which should be restricted from user input:  
  - Users should not be able to enter over-delivery tolerances in purchasing documents;  
  - Users should not be presented with the option of receiving an unlimited over-delivery of goods as this would permit the users’ purchasing authority limits to be exceeded; and  
  - Purchasing users should not be able to determine whether goods receipt transactions are to be performed for the purchase order. These settings should be configured during system implementation and not set within the purchase order. |
**Procurement and payables**

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incomplete purchase orders</td>
<td>Purchase orders that do not contain all of the required data for processing can be blocked (held) from further processing until the required information is entered.</td>
</tr>
<tr>
<td>Follow up of outstanding purchase orders</td>
<td>If specific reminder levels have been specified under the item details of a purchasing document, the system is able to generate reminders and urging letters automatically for unfilled purchase orders. Reminders for non-filled purchase orders and requisitions are defined for purchase value keys.</td>
</tr>
<tr>
<td>Material tolerance</td>
<td>Tolerance key ‘PE’ allows the configuration of a tolerance that checks where the purchase order price differs from the material price held in the material master record.</td>
</tr>
</tbody>
</table>
| Electronic authorisations for purchase requisitions | SAP can be set up to require the electronic authorisation of all purchase requisitions prior to further processing through the use of release strategies:  
  • When a purchase requisition is created, the system should be set up to assign it to a release strategy which requires the document to be released before processing can continue;  
  • The system can be configured to define who is authorised to approve a purchase requisition and in what sequence this should be performed (i.e. purchasing manager followed by the financial controller); and  
  • The system should also be set to control whether a change is allowed during or after the release process and whether a changed document will be subject to a further release procedure as a result. |
| Electronic authorisations for purchase orders | Release strategies can also be defined at the purchase order stage and apply in addition to release at the purchase requisition stage. Purchase order release is performed at the document level only.  
  Consideration may be given to developing an “exit” to bypass the purchase order release stage if the purchase requisition has not been changed since the release of the requisition. |
| Optional automatic generation of purchase orders | Purchase requisitions can be automatically allocated and converted into purchase orders after being approved (released). Purchase orders can then be automatically sent to a vendor (via printer, fax, EDI, etc).       |
2.2 Supplier Relationship Management (SRM)

Functional overview

SRM, previously known as Enterprise Buyer, was developed to allow users to purchase predefined products from approved vendors using an on-line catalogue. Users browse through the on-line catalogue, selecting products and required quantities that are subsequently put into a user’s Shopping Cart.

The SRM process is summarised in the following diagram:

Source: Adapted from information provided by Protiviti Australia
Catalogues available to users may be internal or external. Where external catalogues are available, the approved vendors are allowed to maintain their product listings.

SRM users do not enter prices or material descriptions as these are selected from the catalogue. Most header information for the order is automatically populated by SRM (e.g. vendor information and delivery date which is populated through the use of the vendor info record). The SRM user specifies the deliver-to address from a list of pre-defined and configured deliver-to addresses.

Commonly identified control weaknesses

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basis installation</td>
<td>The SRM system resides on a separate SAP installation to the core SAP system; therefore it requires a separate SAP Basis installation. As a result, in order to appropriately control the SRM environment, Basis settings and parameters should be correctly configured. In addition, the interface between the SRM and SAP ERP core systems should be thoroughly and regularly tested.</td>
</tr>
</tbody>
</table>

**Chapter 5: Basis**

Appropriate Delegation Limits

Configuration control weaknesses identified within the SRM installation are generally related to the configuration of approval delegations. **Appropriate delegation limits** should be configured for SRM transactions. It is important for entities implementing SRM to give consideration to the following through Workflow events:

<table>
<thead>
<tr>
<th>Workflow event condition</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>No approval</td>
<td>Where shopping trolleys are less than an approved amount, Workflow may be configured so that no approval is required. Limits should be applied in line with delegation policy.</td>
</tr>
<tr>
<td>Single approval</td>
<td>Where the shopping trolley amount is greater than the no approval limit, manager approval should be required and configured through Workflow.</td>
</tr>
<tr>
<td>Double approval</td>
<td>Consideration should be given to the application of a double approval step where the value of purchase is above a specified amount. In this case, a line manager and a higher level manager would approve.</td>
</tr>
<tr>
<td>High risk materials</td>
<td>High risk material groups should be configured to require approval, regardless of the dollar value of the goods provided.</td>
</tr>
</tbody>
</table>
Significant risks

High

- Unauthorised purchases are made by SRM users
- Changes are made to orders after approvals have been gained

Medium

- Inappropriate invoices are entered into the system

Segregation of duties risks

- Vendor Maintenance and Bank Reconciliation
- Vendor Maintenance and Purchase Orders
- Vendor Maintenance and Vendor Invoice / Payments

Risks and controls

R206: Unauthorised purchases are made by SRM users

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Approval limits for shopping trolleys, approval levels for shopping trolleys or minimum value of shopping trolleys not requiring approval may be incorrectly configured resulting in unauthorised / inappropriate purchases.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
</tbody>
</table>

- Approval limits configuration (C1026)
  Approval limits should be correctly configured within SRM. Approval limits are assigned to security roles as an attribute. The security roles are then allocated to users who inherit the approval limit assigned to the role. Key areas of configuration include:
  - The no approval limit should be established for small purchases in accordance with the entity’s delegations structure and/or procurement policy;
  - Approval limits should be established in line with the delegation of authorities and organisational structure; and
  - Double approval should be considered for large purchases.

- Manual controls
  - Periodic review of allocation of approval delegations (C1027)
    The allocation of approval delegations to users and / or positions should be regularly reviewed.
R207: Changes are made to orders after approvals have been gained

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Changes to shopping trolleys may be executed following approval resulting in non-authorised procurement of goods.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td>Re-analyse and determine a new release path (C1028)</td>
</tr>
<tr>
<td></td>
<td>When changes are made to approved purchasing orders, SRM should be configured to reanalyse and determine a new release path for the procurement order. Thereby, changed orders will be subjected a second time to pre-determined monetary approvals.</td>
</tr>
</tbody>
</table>

R208: Inappropriate invoices are entered into the system

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Invoice entry is typically performed in the core ERP system. SRM can be used to also process invoices. If SRM is used to process invoices, there is an increased risk of inappropriate access or segregation of duties risks.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td>Segregation of purchasing and invoicing activities (C1029)</td>
</tr>
<tr>
<td></td>
<td>Purchasing and invoicing activities within SRM and between SRM and the SAP ERP core system should be segregated to prevent any fraudulent activity.</td>
</tr>
<tr>
<td></td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td>A periodic review and reconciliation of invoices should be performed in addition to the previously mentioned configuration controls. (C1030)</td>
</tr>
</tbody>
</table>

Security considerations

Consideration should be given to configuration of personalisation settings at an individual or role level. These may include the following:

<table>
<thead>
<tr>
<th>Personalisation Object Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BBP_APPROVAL_LIMIT</td>
<td>Highest value of shopping cart that can be approved</td>
</tr>
<tr>
<td>BBP_SPENDING_LIMIT</td>
<td>Value above which approval is necessary.</td>
</tr>
<tr>
<td>BBP_WFL_SECURITY_BADI</td>
<td>Specifies whether change can be made or what actions should be taken when changes are made to a shopping cart during the approval process. Consideration should be given to forcing the approval process to restart when changes are made.</td>
</tr>
</tbody>
</table>
Restrictions to SRM administration transactions and SRM end user transactions

SRM administration transactions, as well as SRM end user transactions, should be appropriately restricted. These include, but are not limited to:

<table>
<thead>
<tr>
<th>Transaction</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BBPATO3</td>
<td>Create User</td>
<td>SRM transaction used to create a user ID.</td>
</tr>
<tr>
<td>BBPATO4</td>
<td>Forgotten User ID/Password</td>
<td>SRM transaction to request / apply for password and user ID.</td>
</tr>
<tr>
<td>BBP_POC BBP001</td>
<td>Shopping Cart</td>
<td>Create and maintain shopping carts.</td>
</tr>
<tr>
<td>BBPPU05 BBPPU10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BBP_POC_WF_APP</td>
<td>Approve Shopping Cart</td>
<td>Approve shopping cart.</td>
</tr>
<tr>
<td>BBP_POC_WF_REV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BBP_BWS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BBP_BWS_SIMPLE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BBPATO5</td>
<td>Change User Data</td>
<td>Transaction used to change or display SRM user details.</td>
</tr>
<tr>
<td>BBPIV01 BBPIV02</td>
<td>Entry of Invoice</td>
<td>SRM transactions used to enter invoices.</td>
</tr>
<tr>
<td>BBPIV03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BBPPU07</td>
<td>Access to the Managers</td>
<td>SRM transaction used to access the Inbox Manager’s Inbox and related information.</td>
</tr>
<tr>
<td>BBP_BW_SC3 BBP_BW_SC4</td>
<td>Shopping Carts per product or per Cost Centre</td>
<td>Business Warehouse reports used to display summarised shopping cart information.</td>
</tr>
</tbody>
</table>
Common segregation of duties areas of concern

A key difference in assessing segregation of duties with the SRM system is that cross system segregation of duties analysis should be performed. Given that elements of the purchasing process occur within both the core ERP system and SRM, there are incompatible functions that should be segregated across these two systems.

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRM – Create or maintain shopping cart</td>
<td>SRM – Approve shopping cart</td>
<td>The ability to create and approve purchasing transactions may result in unauthorised payments to vendors.</td>
</tr>
<tr>
<td>ERP – Vendor Maintenance</td>
<td>SRM – Create or maintain shopping cart</td>
<td>Could create a fictitious vendor and purchase, resulting in an unauthorised payment.</td>
</tr>
<tr>
<td>ERP – Vendor Maintenance</td>
<td>SRM – Approve shopping cart</td>
<td>Could create a fictitious vendor and purchase, resulting in an unauthorised payment.</td>
</tr>
<tr>
<td>ERP – Invoice Entry</td>
<td>SRM – Create or maintain shopping cart</td>
<td>Could create an unauthorised purchase and process the corresponding payment resulting in inappropriate vendor payment.</td>
</tr>
<tr>
<td>ERP – Invoice Entry</td>
<td>SRM – Approve shopping cart</td>
<td>Could approve an inappropriate purchase and process the corresponding payment, resulting in inappropriate vendor payment.</td>
</tr>
<tr>
<td>ERP – Goods Receipt</td>
<td>SRM – Create or maintain shopping cart</td>
<td>Could purchase an attractive item, receipt the item and misappropriate it.</td>
</tr>
<tr>
<td>ERP – Goods Receipt</td>
<td>SRM – Approve shopping cart</td>
<td>Could approve the purchase of an attractive item, receipt the item and misappropriate it.</td>
</tr>
</tbody>
</table>
Optimising the SAP control environment

Table: Optimising SAP controls

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined fields / Defined attributes</td>
<td>Fields, or attributes, to appear on SRM screens should be defined. This will include defining the user groups and activities that can be performed for each of the fields (for example, define that the requester can ‘change’ the deliver-to address).</td>
</tr>
<tr>
<td>Mandatory key fields</td>
<td>Key fields to be completed should be configured as mandatory to ensure all relevant information is captured. This will ensure that data is available to create relevant purchasing documents.</td>
</tr>
<tr>
<td>Configured product catalogues</td>
<td>Product catalogues should be configured to ensure that users are able to appropriately select from approved internal or external sources.</td>
</tr>
<tr>
<td>Configured workflow</td>
<td>Workflow should be configured to ensure that appropriate approval processes are triggered when a SRM transaction is executed.</td>
</tr>
<tr>
<td>Deliver-to-addresses configured</td>
<td>Deliver-to-addresses should be configured to ensure goods are only delivered to pre-approved delivery points.</td>
</tr>
<tr>
<td>Configured output</td>
<td>Output from the execution of SRM transactions should be configured. For example, purchase orders may be automatically generated following the entry and approval of a SRM transaction. Alternatively, purchase requisitions may be generated and require a purchasing officer to create the purchase order.</td>
</tr>
<tr>
<td>Payment terms</td>
<td>Payment terms configured in the SRM system should correspond with those defined in the core SAP system to ensure that there are no inconsistencies.</td>
</tr>
</tbody>
</table>
2.3 Vendor Master File

Functional overview

The vendor master file is used to store information about each of the vendors that the entity purchases materials or services from. Data is stored at three levels in the vendor master file:

- General data that relates to every company code and purchasing entity;
- Company code / accounting data that is specific to each company code; and
- Purchasing data that is used in the raising of purchasing documents.

Effective and authorised maintenance of vendor master records is critical from a security and control perspective. Master records contain critical data elements, including the vendor bank account which is used for automatic payment, and control key elements, such as whether the duplicate invoice check is performed for each individual vendor.

Commonly identified control weaknesses

The following control weaknesses typically occur in the vendor master file.

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor master data integrity concerns</td>
<td>Vendor records are often created without key fields, for example, the vendor address or telephone number not being populated.</td>
</tr>
<tr>
<td>Use of the alternate payee function</td>
<td>The alternative payee function can result in the processing of payments to a supplier that does not exist on the master file. This function is often not effectively secured.</td>
</tr>
<tr>
<td>Duplicate vendor records</td>
<td>SAP provides an automatic check to identify potential duplicate vendor records. This message is not configured by default and, if not configured, can result in duplicate vendor records in the master file.</td>
</tr>
<tr>
<td>Failure to set the duplicate invoice check</td>
<td>The duplicate invoice check flag in the vendor master record should be mandatory to ensure that duplicate checking is activated for all vendors.</td>
</tr>
<tr>
<td>Inappropriate or unauthorised changes to vendor records</td>
<td>A very useful vendor master record control is the requirement of dual authorisation when changes are made to sensitive fields. This control is rarely implemented, increasing the risk of unauthorised changes being made to vendor records.</td>
</tr>
<tr>
<td>Use of one-time vendor (OTV) function</td>
<td>SAP provides one-time vendor functionality to reduce administration over the vendor master file by paying infrequent vendors through a one-time vendor account. Entities using this function often fail to recognise that it increases the risk of unauthorised payments.</td>
</tr>
</tbody>
</table>

It is common for government entities to use the OTV function for processing of grants payments. In such cases, it is also important to ensure that segregation of duties is maintained between initiating the payment and authorising the payment.
Significant risks

High
- Unapproved or incorrect changes are made to vendor records
- Inappropriate use of the alternative payee function
- Vendor records are not allocated to a reconciliation account

Medium
- Duplicate vendor records are created
- Incorrect payments are made through one-time vendor accounts

Segregation of duties risks
- Vendor Maintenance and Bank Reconciliation
- Vendor Maintenance and Purchase Orders
- Vendor Maintenance and Vendor Invoice / Payments

Risks and controls

R209: Unapproved or incorrect changes are made to vendor records

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Changes to the vendor master file may be made without appropriate approval. Inappropriate changes to sensitive fields, such as those relating to vendor bank account details, can result in the processing of unauthorised or fraudulent expenditure. Failure to populate key vendor master file records can result in master data integrity problems.</td>
</tr>
</tbody>
</table>
| Controls | Configuration controls
- Populate key fields
  To maintain the integrity of vendor records it is important to populate key fields including terms of payment, vendor name and address. (C37)
- Dual authorisation
  SAP provides the ability to require dual authorisation for changes made to sensitive fields. This control can be implemented to ensure that approval is required for all changes to key vendor master record fields. (C39)
- Manual controls
  Review Masterfile Change Report
  There is a Masterfile Change Report (RFKABL00) that may be used to review changes made to vendor records. (C681) |
Eliminating vendor maintenance, segregation of duties concerns using dual control for sensitive fields

SAP provides the ability to require dual authorisation for changes made to sensitive fields. Sensitive fields include items such as bank account changes in a vendor record. If a field in the vendor master record is defined as “sensitive”, the corresponding vendor account is blocked for payment if the entry is changed.

The block is removed when a second person with authorisation checks the change and confirms or rejects it. The approval process is performed through transaction FK08 and FK09.

Entities often experience difficulties with segregation of duties issues, particularly concerning the vendor maintenance function. Although remediation of the segregation of duties is made a priority, changes to the overall security environment or changes that require job functions to be segregated may take a longer implementation period.

To mitigate the segregation of duties risk, entities should consider implementing the dual authorisation control for key vendor maintenance fields. The advantage of this control is that SAP will not allow the same person who made the change to the vendor record to approve the change.

Source: Protiviti Australia

R210: Inappropriate use of the alternative payee function

| Risk rating | HIGH |
| Risk description | The alternative payee in document is a field that may be checked within vendor master records and which may be set at either the overall vendor level, which would apply to all company codes, or for a specific company code. The document field setting would be set at the overall level if it is desirable to maintain it for the entire vendor record across companies, otherwise it should be set for each individual company.

This is a significant risk in processing payments to incorrect or fraudulent bank accounts or vendors. The risk level is high, particularly where at the overall level, any payee is able to be entered. |
| Controls | Configuration controls
1. Alternative payee field
The alternative payee field at the overall vendor relates to the overall vendor account, the company code field is relevant when the vendor account is extended to each company code within the entity. It is important that the overall and company code alternative payee field is suppressed. (C801) (C802) |
### R211: Vendor records are not allocated to a reconciliation account

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Vendor accounts should be defined as reconciliation accounts to restrict the ability to post manual entries in the General Ledger. Failure to set a vendor account as a reconciliation account may result in reconciling problems between the General Ledger and the Accounts Payable sub-ledger.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>Definition of reconciliation accounts (C220)</strong></td>
</tr>
<tr>
<td></td>
<td>Reconciliation accounts should be defined to ensure integrity between the general ledger and the accounts payable sub-ledger. Each vendor (sub-ledger) account should then be attached to the reconciliation account. Direct posting to the reconciliation account is then automatically blocked.</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter 5: Controlling</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Chapter 3: General Ledger</strong></td>
</tr>
</tbody>
</table>

### R212: Duplicate vendor records are created

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Duplicate vendor master records may exist which could be used to process unauthorised or fraudulent transactions.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>Duplicate vendor check (C600)</strong></td>
</tr>
<tr>
<td></td>
<td>SAP provides the ability to identify potential duplicate vendor records as they are processed. The duplicate vendor check is not set by default. To enable this check, the system message for duplicate vendors should be set as a warning (cannot be set as an error).</td>
</tr>
</tbody>
</table>
## R213: Incorrect payments are made through one-time vendor accounts

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk description</strong></td>
<td>SAP provides one-time vendor functionality to reduce administration over the vendor master file by paying infrequent vendors through a one-time vendor account. The use of the one-time vendor function overcomes typical vendor master file authorisation and review controls and may be used to process unauthorised payments. For government entities using the OTV function for processing grants payments and where such payments are a material financial reporting item, this risk may be rated as HIGH.</td>
</tr>
<tr>
<td><strong>Controls</strong></td>
<td>Manual controls</td>
</tr>
</tbody>
</table>

   1. **Periodically review one-time vendor (OTV) payments (C41)**

Use of the one-time vendor function eliminates typical vendor master file controls, including vendor approval, vendor tolerances, and standard terms of payment. To reduce the risk associated with the use of this function, it is important to periodically review one-time vendor payments. The vendor line item report RFKEPL00, transaction code S_ALR_87012103, is the best report to view one-time vendor payments. Payments are also be viewed through the Purchasing Overview by Vendor Report.

---

### One-time vendor (OTV) payments

It is common for entities to implement the use of one-time vendor payments to reduce overhead in the Accounts Payable area. It is associated with the set up of infrequent vendors on the vendor master file.

Entities that use OTV payment increase the risk that the OTV process is being used to pay vendors multiple times, rather than for simply paying infrequent use vendors.

To eliminate this risk, entities should reduce the number of one-time vendor accounts that they use and implement periodic reviews of policies/procedures for use of OTV.

Source: Protiviti Australia
Security considerations

Standard vendor master security transactions and authorisation objects that should be restricted to appropriate master data staff

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td>Description</td>
</tr>
<tr>
<td>XK01, FK01, MK01</td>
<td>Create Vendor</td>
</tr>
<tr>
<td>XK02, FK02, MK02</td>
<td>Change Vendor</td>
</tr>
<tr>
<td>FK08</td>
<td>Confirm Vendor Changes Individually</td>
</tr>
<tr>
<td>FK09</td>
<td>Confirm Vendor Changes List</td>
</tr>
</tbody>
</table>

Authorisation Objects

| F_LFA1_BUK                   | Vendor: Authorisation for Company Codes          |
| F_LFA1_AEN                   | Vendor: Change Authorisation for Certain Fields  |
| F_LFA1_GRP                   | Vendor: Account Group Authorisation              |
| F_LFA1_BEK                   | Vendor: Account Authorisation                    |

Entity Values

| BUKRS                        | Company Code                                     |

Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Maintenance</td>
<td>Bank Reconciliation</td>
<td>Users may change vendor account details and perform an incorrect or fraudulent bank/check reconciliation to hide entries related to those vendor accounts.</td>
</tr>
<tr>
<td>Vendor Maintenance</td>
<td>Purchase Orders</td>
<td>A user may be able to create a fictitious/unauthorised purchase order for a fictitious/unauthorised vendor in order to conceal the payment or to provide business to a preferred unauthorised vendor.</td>
</tr>
<tr>
<td>Vendor Maintenance</td>
<td>Vendor Invoice / Payments</td>
<td>A user could create a ghost vendor or change an existing vendor’s bank account and direct an existing invoice for payment. In addition, a user may create a fictitious vendor or collude with an existing vendor to receive unauthorised discounts and payments, resulting in misappropriation of payment funds.</td>
</tr>
</tbody>
</table>
Optimising the SAP control environment

The following items should be considered to enhance the maintenance of the vendor maintenance function.

### Optimising SAP controls

- Vendor payment terms
- Vendor payment block
- Reports for review
- Evaluated receipt settlement

### Area | Description
--- | ---
Vendor payment terms | Payment terms are specific agreements with customers on how invoices are to be paid. For example, net due in 30 days or 2% discount if paid within 10 days. They should be assigned to each vendor when it is created. When an order is placed with the vendor, the terms of payment automatically appear as default values. Payment terms should be configured as a required entry field for the creation of vendor master records and should not be changed during purchase order entry or invoice processing.

Vendor payment block | Individual vendor accounts can be blocked for payment by applying the relevant payment block in the vendor master record. Procedures should be implemented to ensure that vendor accounts are blocked where necessary and that any changes to vendor master record payment blocks are reviewed.

Reports for review | The following reports should be used for periodic review and reconciliation:
- **Display of vendor changes** – Report RFKEPL00, transaction code S_ALR_870012089 – this report provides a list of vendor master records that have been changed. It shows the original and changed fields and values as well as details on which user performed the changes;
- **List of new vendors** – Report RFKKVZ00, transaction code S_ALR_87012086 – this report provides details of all new vendor master records created for the selected date range; and
- **Display of bank account changes** – Report RFKABL00, transaction code S_ALR_87012089 – this report should also be reviewed regularly to ensure that changes made to bank master data are authorised.

 Evaluated receipt settlement | If evaluated receipt settlement (ERS) processing is used, it should be activated in the vendor master record as well as in the purchasing information record (PIR). The system will automatically set all purchasing transactions as ‘ERS-relevant’ during processing. If ERS is deactivated in the PIR or vendor master, ERS will not be performed. Changes to the ERS settings in the vendor master and PIR should be adequately restricted. The report *Changes to purchasing info records* should be regularly reviewed for ERS vendors to ensure that no unauthorised changes are made to PIRs for the vendors. However, this report is limited because it may only provide details of changes for nominated vendors. Consideration should also be given to developing a custom report to highlight changes specifically to ERS indicators for all vendors.
2.4 Material Master File

Functional overview

The material master file is used to store details of materials that are purchased by an entity. A material master record is created for each material. A variety of information can be stored in a material master file, including accounting data, purchasing data, production data, classification details, storage information, quality management information, and work scheduling data. All materials are assigned a material type which determines the valuation and treatment of the material in the system.

It should be noted that inventory management is not within the scope of this guide, however, the material master file is covered briefly to provide a more complete picture of the procurement process.

Commonly identified control weaknesses

The following control weaknesses typically occur in the material master file.

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery tolerances</td>
<td>Appropriate under and over-delivery tolerances should be configured for the purchasing value keys assigned to material master records to prevent excessive over-deliveries.</td>
</tr>
<tr>
<td>Negative stock</td>
<td>Negative stocks should be disabled, unless specifically required for a particular material type.</td>
</tr>
<tr>
<td>Valuation methods</td>
<td>The correct valuation method should be assigned to each material item.</td>
</tr>
<tr>
<td>Source lists</td>
<td>A source of supply for each material should be maintained for source lists.</td>
</tr>
</tbody>
</table>

Significant risks

- **High**
  - Material master integrity concerns including valuation issues
  - Inventory balances recorded in the material master do not exist

- **Medium**
  - Duplicate material items exist
Risks and controls

### R214: Material master integrity concerns including valuation issues

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>The material master is critical for the accurate recording of inventory balances and valuation in the General Ledger. Failure to assign the correct valuation method or incorrectly configure inventory items to allow negative items will impact the accuracy of the inventory balance maintained within the financial statements.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Controls</th>
<th>Configuration controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Price control</td>
</tr>
<tr>
<td></td>
<td>It is possible to make price control either standard or moving average price mandatory for all material master records. (C500)</td>
</tr>
<tr>
<td></td>
<td>Setting material pricing</td>
</tr>
<tr>
<td></td>
<td>Material pricing should be set on each material type. There are two options S – Standard Pricing and V – Moving Average Pricing. (C492)</td>
</tr>
<tr>
<td></td>
<td>Permission of negative stock balances</td>
</tr>
<tr>
<td></td>
<td>It is possible to configure whether negative stock balances are permitted. It is also possible to configure whether negative stocks are permitted by company code and valuation area. (C284)</td>
</tr>
<tr>
<td></td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td>Periodically review changes to material master records. The report SAPMM03A, transaction code MM04, Display Material Change Documents, can be viewed by material, plant, a specific user or a selected period. This report can be accessed through transaction MM04. (C627)</td>
</tr>
</tbody>
</table>

### R215: Inventory balances recorded in the material master do not exist

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Recorded inventory items may not exist, incorrectly inflating the inventory balance in the General Ledger resulting in financial misstatement.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Controls</th>
<th>Manual controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cycle counting</td>
</tr>
<tr>
<td></td>
<td>Cycle counting is a method of managing physical inventory whereby inventory is counted at regular intervals within a fiscal year. Cycle counting allows for the counting of fast-moving items more frequently than slow moving items. (C289)</td>
</tr>
<tr>
<td></td>
<td>Performance of inventory stock takes</td>
</tr>
<tr>
<td></td>
<td>If SAP cycle counting or inventory sampling is not used, traditional stock takes should be performed on a periodic basis. (C278)</td>
</tr>
</tbody>
</table>
R216: Duplicate material items exist

Risk rating | MEDIUM
---|---
Risk description | Duplicate materials could be maintained, resulting in mismanagement of inventory and financial cost to the entity.

Controls | Manual controls
---|---
Procedures in place to review material master files
When creating new material items, it is important that strict procedures are put in place to review material master files. This will help ensure the inventory item does not already exist. (C274)

Security considerations

Authorisation groups can be assigned to material types to provide an additional level of security. Consideration should also be given to restricting access to particular views of the material master records. It is also possible to restrict access to particular fields in the material master records via the use of ‘field groups’.

Standard material master security objects that should be restricted to appropriate master data staff

<table>
<thead>
<tr>
<th>Security Items</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td></td>
</tr>
<tr>
<td>MM01</td>
<td>Create Material</td>
</tr>
<tr>
<td>MM02</td>
<td>Change Material</td>
</tr>
<tr>
<td>MM04</td>
<td>Display Material Change Documents</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>M_MATE_BUK</td>
<td>Material Master: Company Codes</td>
</tr>
<tr>
<td>M_MATE_WRK</td>
<td>Material Master: Plants</td>
</tr>
<tr>
<td>M_MATE_MAR</td>
<td>Material Master: Material Types</td>
</tr>
<tr>
<td>Entity Values</td>
<td></td>
</tr>
<tr>
<td>WERKS</td>
<td>Plant</td>
</tr>
<tr>
<td>BUKRS</td>
<td>Company Code</td>
</tr>
</tbody>
</table>
Optimising the SAP control environment

<table>
<thead>
<tr>
<th>Optimising SAP controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Purchasing value keys</td>
</tr>
<tr>
<td>• Source lists</td>
</tr>
<tr>
<td>• Expiration date settings</td>
</tr>
</tbody>
</table>

The following items should be considered to ensure material information is entered accurately and correctly:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchasing value keys</td>
<td>Purchasing value keys should be defined in the system and assigned to individual material master records to control the acceptable limits for under- and over-delivery tolerances. Tolerances should be set at a reasonable level and no material master records should be set to accept unlimited over-deliveries.</td>
</tr>
<tr>
<td>Source lists</td>
<td>For materials that should only be purchased via a source list, the appropriate indicator should be set to prevent purchases other than via the source list.</td>
</tr>
<tr>
<td>Expiration date settings</td>
<td>It is possible to define whether SAP performs an expiration date check for inventory items.</td>
</tr>
<tr>
<td></td>
<td>It is possible to activate expiration checking for individual plant locations.</td>
</tr>
</tbody>
</table>
2.5 Receipt of goods or services

Functional overview

When the goods ordered via a purchase order are received, a goods movement is processed in the system. The purchase order number is entered and this automatically transfers the details into the goods receipt document, allowing the user to make changes to account for the actual quantities received.

An effective goods receipt process is critical to ensure that payments are only processed when goods have been received and are in good condition.

Commonly identified control weaknesses

The following control weaknesses typically occur in the goods receipt process:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason codes</td>
<td>Often reason codes are not effectively customised to define and enforce the reasons for return/write-off transactions.</td>
</tr>
<tr>
<td>Purchasing value keys</td>
<td>Purchasing value keys should not be configured correctly to disallow excessive over-deliveries. By default one of the purchase value keys delivered by SAP allows for unlimited over-delivery; this purchase value key is often allocated to either material items or vendor accounts.</td>
</tr>
</tbody>
</table>

Significant risks

- **High**
  - Unapproved or incorrect purchase requisitions are created
  - Goods receipt quantity differs from ordered quantity

- **Medium**
  - Damaged goods are accepted

- **Segregation of duties risks**
  - Goods Receipt and AP Invoice Entry
  - Goods Receipt and Purchase Document Entry or Approval
  - Goods Receipt and Asset Master Maintenance
  - Goods Receipt and Material Master Maintenance
  - Goods Receipt and Vendor Maintenance
  - Service Master Maintenance and Service Acceptance
## Risks and controls

<table>
<thead>
<tr>
<th>R217: Unapproved or incorrect purchase requisitions are created</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk rating</strong></td>
<td>HIGH</td>
</tr>
<tr>
<td><strong>Risk description</strong></td>
<td>The goods receipt indicator is not selected when processing purchase requisitions or orders. Failure to set this indicator can impact on the integrity of the three way match approval process, resulting in over-delivery and/or over payments for goods or services.</td>
</tr>
<tr>
<td><strong>Controls</strong></td>
<td><strong>Configuration controls</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Set goods receipt indicator</strong></td>
</tr>
<tr>
<td></td>
<td>The goods receipt indicator is a critical field. Where selected it requires the entry of two critical invoice verification fields: GR, which links the goods receipt to the purchase item; and IR, which links the invoice receipt to the purchase item. The goods receipt indicator should be a required field. The GR-based IV field ensures that provision is made for goods receipt based invoice verification. Where selected it ensures that individual purchase items are matched to the goods receipt. (C829) (C830)</td>
</tr>
</tbody>
</table>
### R218: Goods receipt quantity differs from ordered quantity

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>SAP should be effectively configured to restrict the ability to over or under deliver for specified purchase order items. Over deliveries are incorrectly accepted. This could result in increased inventory items.</td>
</tr>
<tr>
<td>Controls</td>
<td><strong>Configuration controls</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Set order price tolerance</strong></td>
</tr>
<tr>
<td></td>
<td>An order price tolerance (B1 or B2) can be set within SAP for over or under deliveries. SAP checks each goods receipt item to determine whether it varies from the purchase order item. This tolerance is used where the order unit (i.e. quantity) is not the same as the costing unit (i.e. weight or volume). A warning or error can be identified when the tolerance is exceeded. (C247)</td>
</tr>
<tr>
<td></td>
<td><strong>Set accuracy of payments relating to a goods receipt tolerance</strong></td>
</tr>
<tr>
<td></td>
<td>A tolerance should be set to measure the accuracy of payments relating to a goods receipt. This tolerance is extremely useful as it allows high quantity variances for invoices with small amounts and only small quantity variances for invoice items with large amounts. Both upper and lower percentage limits can be established. (C479)</td>
</tr>
<tr>
<td></td>
<td><strong>Setting appropriate purchase value keys</strong></td>
</tr>
<tr>
<td></td>
<td>Purchase value keys define a number of key criteria for the processing of purchase orders. They are allocated to either material items or directly to purchase orders. Appropriately setting purchase value keys on material and purchase order items is important to minimise the risk of over and under delivery. (C505)</td>
</tr>
</tbody>
</table>

### R219: Damaged goods are accepted

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Goods receipt procedures may not be sufficient to ensure goods are inspected for quality and any damaged goods identified and returned. This can lead to the receipt of damaged goods, resulting in financial loss to the entity.</td>
</tr>
<tr>
<td>Controls</td>
<td><strong>Manual controls</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Goods receipt procedures</strong> are required to define processes that should be followed when receipting goods and services into the SAP system. Goods receipt procedures should define whether over deliveries are to be accepted and include processes for inspecting the quality of shipments. (C248)</td>
</tr>
</tbody>
</table>
Security considerations

The MIGO (Goods Movement) transaction may be used to input all types of goods movements in the system. Therefore, all users should be provided with access to only those movement types required to perform their duties. No users should be allocated movement types which allow for the processing of a goods receipt without reference to a purchase order.

Standard goods receipt security objects that should be restricted

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td></td>
</tr>
<tr>
<td>MIGO</td>
<td>Goods Movement</td>
</tr>
<tr>
<td>MB01</td>
<td>Goods Receipt for a Purchase Order</td>
</tr>
<tr>
<td>MB11</td>
<td>Goods Movement</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>M_MSEG_WWE</td>
<td>Goods Receipt for Purchase Order: Plant</td>
</tr>
<tr>
<td>M_MSEG_BWE</td>
<td>Goods Receipt for Purchase Order: Movement Type</td>
</tr>
<tr>
<td>Entity Values</td>
<td></td>
</tr>
<tr>
<td>WERKS</td>
<td>Plant</td>
</tr>
</tbody>
</table>
## Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goods Receipt</td>
<td>AP Invoice Entry</td>
<td>The requirement for independent receipt of goods or services reduces the risk that a single staff person may process a fraudulent payment and then hide the payment through incorrect goods receipt.</td>
</tr>
<tr>
<td>Goods Receipt</td>
<td>Purchase Document Entry or Approval</td>
<td>Enter or approve a purchase document and process a fictitious goods receipt or under receipt the inventory item and misappropriate the goods.</td>
</tr>
<tr>
<td>Goods Receipt</td>
<td>Asset Master Maintenance</td>
<td>A user could create an asset record, process a goods receipt to record the asset, and then misappropriate the asset.</td>
</tr>
<tr>
<td>Goods Receipt</td>
<td>Material Master Maintenance</td>
<td>User may enter incorrect goods receipt information and modify inventory levels accordingly. This may result in the misappropriation of assets.</td>
</tr>
<tr>
<td>Goods Receipt</td>
<td>Vendor Maintenance</td>
<td>User may enter incorrect goods receipt information including changing the delivery address for attractive items and modify vendor master data accordingly. The goods may then be receipted into SAP and misappropriated.</td>
</tr>
<tr>
<td>Service Master Maintenance</td>
<td>Service Acceptance</td>
<td>Create service master records and process incorrect acceptance, resulting in an incorrect payment.</td>
</tr>
</tbody>
</table>

## Optimising the SAP control environment

**Optimising SAP controls**

- Assess the use of standard SAP Goods Receipt Movement Types
- GRIR report review
- Service acceptance
- Reversals of goods receipt
The following better practice items should be considered to improve the goods receipting process:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess the use of standard SAP Goods Receipt Movement Types</td>
<td>Movement types determine the type of inventory movement recognised by SAP and the corresponding accounting, including which quantity fields, stock types and General Ledger accounts are updated. Movement types should be appropriately configured to ensure that the correct accounting entries are generated. If a valid purchase order number does not exist in the system, a delivery is input to the system using a special ‘movement type’. Use of this movement type should be restricted via SAP security and its use monitored, as it allows the matching controls to be bypassed. Various movement types defined in the system allow the initial entry of stock balances and are intended for use only as part of the data load from legacy systems. After conversion, access to these movement types (which do not generate the standard financial entries) should be prohibited.</td>
</tr>
<tr>
<td>GR/IR report review</td>
<td>The GR/IR Clearing Accounts Analysis and List of GR/IR Balances reports should be reviewed periodically to ensure that any unmatched invoices (i.e. if the goods receipt has been omitted) are followed up.</td>
</tr>
<tr>
<td>Service acceptance</td>
<td>There is no separate document in SAP for the acceptance of services actually performed. The ‘service entry sheet’ is checked for accuracy by the person responsible and then released (accepted) for invoice processing purposes. SAP security should be set up to segregate the entry and acceptance functions so that one person is authorised to enter services performed and another is authorised to accept them. This effectively provides an electronic authorisation of the services for payment.</td>
</tr>
<tr>
<td>Reversals of goods receipt</td>
<td>Where ‘goods-receipt-based invoice verification’ is being used, the system should be configured to ensure that a reversal cannot be processed for a goods receipt when the invoice has already been processed. Otherwise the invoice matching process may be compromised. Appropriate procedural controls should be in place to control the processing of reversal entries. Reversal of goods receipt transactions should only be processed on the basis of authorised requests. Consideration should also be given to producing an exception report of all goods receipt reversals for management review. The return delivery should reference the purchase order or the material document so that the system properly reference and reverse the original data.</td>
</tr>
</tbody>
</table>
2.6 Invoice Processing

Invoice verification overview

Invoice verification is the process of entering invoices for payment of purchasing documents, including purchase orders and requisitions. Invoice details are matched to the purchase order and goods receipt details. However, further configuration controls may also be implemented that verify the invoice simply against the goods receipt details. Differences in the document values outside of set tolerances result in the invoice being blocked for payment.

Evaluated Receipt Settlement (ERS) involves the settlement of goods receipts without receiving an invoice. Payment is generated based on the order price specified in the purchase order and the quantity entered on the goods receipt. ERS is regularly used to improve the efficiency of the Accounts Payable process.

Invoices may also be processed directly via the Financial Accounting Accounts Payable function. These invoices are not matched to purchase order and goods receipt details. This function is used to process invoices for which no purchase order has been raised (i.e. utility payments).
Commonly identified control weaknesses

Control weaknesses that typically occur in processing Accounts Payable invoices

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inconsistent invoice tolerances</td>
<td>Tolerances should be configured to ensure that significant variations between the purchase order, goods receipt and invoice are blocked. There are a number of key tolerances that should be configured. Often, these tolerances are not set correctly.</td>
</tr>
<tr>
<td>Failure to set the duplicate invoice check</td>
<td>The default duplicate invoice check is only performed for a vendor if it is enabled in the vendor record. Entities do not always make the duplicate invoice check a required field.</td>
</tr>
<tr>
<td>Ability to process non-order invoices through invoice verification</td>
<td>Tolerance key AN is able to be configured to limit the ability to process invoices through invoice verification that do not reference to a purchase order. This tolerance is rarely implemented.</td>
</tr>
<tr>
<td>Payment of unauthorised direct entry invoice payments</td>
<td>Invoice verification invoices are typically better controlled than direct entry invoices since they are approved by release strategies, whereas reliance is placed on manual approval for direct entry invoices. Most entities do not have adequate assurance that direct entry invoices have been adequately approved in accordance with the entity’s approval delegations.</td>
</tr>
</tbody>
</table>

Significant risks

- **High**
  - Duplicate invoices are processed
  - Unapproved or incorrect non-order invoices are created
  - Incorrect purchase order payments are processed
  - Goods Receipt (GR) / Invoice Receipt (IR) account is not adequately reconciled

- **Medium**
  - Parked and blocked invoices are not actioned
  - Returned goods are still invoiced
  - Inappropriate changes are made to invoices after processing

- **Segregation of duties risks**
  - Invoice Entry and Invoice Release
  - Invoice Entry and Vendor Payments
  - Invoice Entry and Purchase Document Approvals
  - Invoice Entry and Vendor Maintenance
Risks and controls

R220: Duplicate invoices are processed

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Duplicate invoice payments may be processed, resulting in financial loss for the entity.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
</tbody>
</table>

**Warning configuration** – SAP can be configured to provide the user with a warning whenever a potential duplicate invoice is processed. The duplicate invoice check is a field in the vendor master record. This field should be selected to enable duplicate invoice checking for the vendor, therefore, the field should be a required field in all vendor account groups. (C252)

**Manual controls**

**Periodically review potential duplicate invoice payments**

A periodic review of duplicate invoice payments should be performed and all potential duplicate invoice payments should be followed up and actioned appropriately. (C617)

**Duplicate invoice check**

An entity issued a purchase order for ten new executive desks. The vendor supplied the first six desks and invoiced for them. The entity processed the invoice and issued payment for the six desks.

However, when the remaining four desks were delivered, the vendor mistakenly invoiced for all ten desks. The purchasing department entered the invoice into SAP and payment was issued for the full allotment of ten desks, creating an overpayment for six additional desks and costing the entity $10,000.

Duplicate invoices are a serious risk to an entity’s financial wellbeing. The business cannot rely on a vendor’s processes to catch and report back any duplicate or over-payments to the payer. Therefore, the entity should take preventive action to avoid the overpayment of invoices.

If automatic duplicate invoice checking had been activated in this scenario, at the time of the second invoice’s entry, SAP could have automatically checked the invoice against the vendor, the referenced purchase order, and the outstanding balances. The system would have produced an error or warning that would require further investigation by the Accounts Payable clerk.

Source: Protiviti Australia
### R221: Unapproved or incorrect non-order invoices are created

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
</table>
| Risk description | Direct entry invoices or non-order invoices are a key risk in SAP, as these types of invoices do not typically have robust automated approval controls operating over them. It is important that all non-order invoices are correctly authorised.  
Non-order invoices may be processed through invoice verification without reference to a purchase order, thereby avoiding three way match controls and increasing the risk of unauthorised payments or overpayments. |
| Controls | **Configuration controls**  
**Automated approval**  
There are a number of ways that automated approval can be implemented over direct entry invoices. These include the use of workflow, using the SAP default ‘park and post’ functionality or through the use of the stochastic block. (C1032)  

| 1 | Restrict ability to process non-purchase order invoices tolerance  
SAP provides the ability to enter an invoice through invoice verification which does not reference to an approved purchase order. Tolerance key AN should be enabled to restrict the ability to process and invoice through SAP transaction MIRO that is not related to a purchase order. (C466) |
| Manual controls | **Appropriate approval**  
All direct entry invoices should be appropriately approved in accordance with delegation of authority. (C1033) |
### R222: Incorrect purchase order payments are processed

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>An incorrect purchase order invoice amount could be paid. The process to follow up and action mismatches from the three way process may be inadequate, resulting in the processing of over payments.</td>
</tr>
</tbody>
</table>

**Controls**

**Configuration controls**

*Define and configure the ‘PP’ tolerance*

SAP provides the ‘PP’ tolerance, which determines by how much each invoice item varies from the product of quantity invoiced multiplied by the order price. For the processing of invoices that relate to a purchase order, the PP tolerance should be defined for the entity. The tolerances should be appropriately configured to minimise the number of inaccurate disbursements while reducing the number of blocked payments due to unmatched invoices (against the purchase order or receiving document). (C619)

**Manual controls**

*Follow up of blocked for payment invoices*

Processes should be put in place to follow up invoices that are blocked for payment as a result of a tolerance block. In addition, Accounts Payable should regularly review price and quantity tolerances. (C251)

### R223: Goods Receipt (GR) / Invoice Receipt (IR) account is not adequately reconciled

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>The GR/IR account identifies timing differences between the receipt of goods and the receipt of an invoice, and should be periodically cleared using the FI clearing program. The GR/IR account may not be monitored regularly to ensure goods receipts and invoice receipts are matched and processed on a timely basis, typically weekly. Since this account tracks differences between goods receipts and invoices, goods receipts with no corresponding invoices, or invoices with no corresponding goods receipts, it is crucial that it be properly monitored.</td>
</tr>
</tbody>
</table>

**Controls**

**Manual controls**

*Reconciliation of goods receipt not invoiced account*

The goods received not invoiced account should be reconciled to understand future payment commitments. (C253)
<table>
<thead>
<tr>
<th>R224: Parked and blocked invoices are not actioned</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk rating</strong></td>
</tr>
<tr>
<td><strong>Risk description</strong></td>
</tr>
</tbody>
</table>
| **Controls** | **Configuration controls**  
*Determiniation of payment block removal*  
Payment block reasons are allocated to Accounts Payable document types. The purpose of allocating payment blocks is to restrict processing of sensitive payment types without subsequent approval. When establishing payment blocks, it can be determined whether the block can be removed during payment processing or when processing manual payments. If payment blocks have been set for a particular document type, it is important that the block cannot be removed via a manual payment or during payment processing. (C263)  
**Manual controls**  
*Identification of parked or blocked invoices*  
Transaction FBV3 should be used to identify parked or blocked invoices. The transaction can be run for either a company code or a fiscal year. (C257) |

<table>
<thead>
<tr>
<th>R225: Returned goods are still invoiced</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk rating</strong></td>
</tr>
<tr>
<td><strong>Risk description</strong></td>
</tr>
</tbody>
</table>
| **Controls** | Goods return procedures should be developed and followed. Key controls that should be included in the process include:  
**Configuration controls**  
*Processing of returned goods*  
SAP should be used to process all goods returns. A reason for the goods return should be recorded in the system. (C249)  
**Manual controls**  
*Notification processes* should exist to identify where goods are not successfully returned to vendors. (C1034)  
Policies and procedures should include, for example, the notification of the Accounts Payable section to ensure that goods that have been returned are not paid for by the entity. (C1035) |
R226: Inappropriate changes are made to invoices after processing

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Document change rules have been incorrectly set up, resulting in the ability to incorrectly change invoice records, particularly one-time vendor items after posting.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td>Alteration of default document change rules</td>
<td></td>
</tr>
</tbody>
</table>

Document change rules define the circumstances by which fields may be changed after posting. By default, there are a number of one-time vendor fields that may be altered. Default document change rules should be altered to restrict the ability to alter key invoice fields. (C701)

Security considerations

Standard invoice verification security objects that should be restricted to appropriate staff

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transactions</strong></td>
<td></td>
</tr>
<tr>
<td>MIRO</td>
<td>Enter Invoice Verification Invoice</td>
</tr>
<tr>
<td>MR01</td>
<td>Process Incoming Invoice</td>
</tr>
<tr>
<td>MR02</td>
<td>Process Blocked Invoices</td>
</tr>
<tr>
<td>F-43, FB01, FB60</td>
<td>Direct Entry Invoice</td>
</tr>
<tr>
<td><strong>Authorisation Objects</strong></td>
<td></td>
</tr>
<tr>
<td>M_RECH_BUK</td>
<td>Invoices: Company Code</td>
</tr>
<tr>
<td>M_RECH_EKG</td>
<td>Invoice Release: Purchasing Group</td>
</tr>
<tr>
<td>M_RECH_SPG</td>
<td>Invoices: Blocking Reasons</td>
</tr>
<tr>
<td>F_BKP_BUK</td>
<td>Accounting Document: Authorisation for Company Codes</td>
</tr>
<tr>
<td>F_BKP_BLA</td>
<td>Accounting Document: Authorisation for Document Types</td>
</tr>
<tr>
<td>F_BKP_KOA</td>
<td>Accounting Document: Authorisation for Account Types</td>
</tr>
<tr>
<td>M_RECH_WRK</td>
<td>Invoices: Plant</td>
</tr>
<tr>
<td><strong>Entity Values</strong></td>
<td></td>
</tr>
<tr>
<td>BUKRS</td>
<td>Company Code</td>
</tr>
<tr>
<td>EKGRP</td>
<td>Purchasing group</td>
</tr>
<tr>
<td>WERKS</td>
<td>Plant</td>
</tr>
<tr>
<td>KOART</td>
<td>Account Type</td>
</tr>
</tbody>
</table>
Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoice Entry</td>
<td>Invoice Release</td>
<td>A user with the ability to process an invoice and then release the invoice may override the three or two way match tolerance settings which cover the adequacy of payments. The risk is also increased where the payment is made to a one-time or alternative vendor account.</td>
</tr>
<tr>
<td>Invoice Entry</td>
<td>Vendor Payments</td>
<td>A user could create a fraudulent invoice and process that payment through the automatic payment program. This is of particular concern where the alternative payee function is available.</td>
</tr>
<tr>
<td>Invoice Entry</td>
<td>Purchase Document Approvals</td>
<td>A user could purchase an item and process the invoice resulting in unauthorised payment. The criticality of this risk is reduced if automated purchasing order approval has been implemented.</td>
</tr>
<tr>
<td>Invoice Entry</td>
<td>Vendor Maintenance</td>
<td>This would result in the processing of fraudulent payments. A user would have the capability to input fraudulent purchase orders or non-invoices and be able to change the vendor’s bank account information to a personal account. Invoices processed through invoice verification are also a risk if key tolerances have not been established correctly.</td>
</tr>
</tbody>
</table>

**OCR invoice scanning**

Entities are increasingly introducing the use of an automated invoice verification system using OCR (optical character recognition) technology. Multiple SAP Certified software solutions are available, including applications from Readsoft, OpenText, and DataCap. The advantages of this technology include a reduction in time, effort and cost to process invoices through the reduction of manual data entry and staff necessary to complete the process.

The software is used to scan or capture invoices and transfer the information into SAP. The supplier information, product data and cost are validated against vendor master data and existing purchase orders. Validated invoices are forwarded to Accounts Payable for posting. Invoices that cannot be validated automatically are sent to a workflow process.

This guide reflects the use of a manual process. However, if an entity has implemented an automated solution, the control themes do not change dramatically. Increased scrutiny should be given to the configuration and interfaces of the tool and corresponding workflows, with a reduced focus on user input.

Source: Protiviti Australia
Optimising the SAP control environment

Optimising SAP controls

- Evaluated receipts settlement
- Stochastic blocking
- Recurring invoices
- OCR invoice scanning

Better practice procedures which may be implemented in the Invoice Entry process include:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
</table>
| Evaluated receipt settlement | Evaluated receipt settlement (ERS) may be used to process payments based on matching of goods receipt and purchase order items.  
In order to use the ERS function, the ERS parameter should be flagged within the purchase order or in the vendor master records. If the vendor is subject to ERS, the system will automatically set all line items as being ERS-relevant. The ERS indicator may be removed for any particular line item.  
If a vendor has been set to ERS, the user is able to set the purchasing info record to non-ERS to prevent ERS processing. The system will not set the ERS indicator on an item if the purchasing info record has been flagged as non ERS. Therefore, access to the purchasing info record should be restricted and a regular review should be performed of any changes to the ERS parameters in the purchasing info record. |
| Stochastic blocking        | SAP can be configured to automatically block a random sample of invoices processed via Accounts Payable. This is referred to as ‘stochastic blocking’ and can be configured to block a specified percentage of all invoices or a percentage of all invoices above a threshold value. |
| Recurring invoices         | Posting of recurring invoices is performed only after running the recurring entries program as specified within the scheduling parameters. Entry of the original recurring document will not update any accounts. Details of the batch run should be reviewed through the program RSBDCSUB to ensure the accuracy and completeness of processing. |
| OCR invoice scanning       | To remove data integrity concerns with invoice entry, and to improve the efficiency of the accounts payable process, optical character recognition software and scanning may be used. |
2.7 Payment Processing

Functional overview

Invoices are processed either via invoice verification (Materials Management) or Accounts Payable (Financial Accounting) and are stored in the system as ‘open items’. If the invoices are not blocked for payment they will be automatically paid via the payment program by the due date. The invoices are then cleared by the payment program. The system can also be configured to take advantage of prompt payment discounts. Payments are output to one of several forms of media, including EDI, bank transfers, and paper cheques. Manual payments can also be processed and manual cheques produced.

Commonly identified control weaknesses

The following control weaknesses typically occur in the Payment processing process.

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
</table>
| Payment blocking                        | Blocking reasons are rarely appropriately configured to prevent direct removal of payment blocks during a payment run or via the manual entry of payments. Payment block reasons are allocated to Accounts Payable document types. The purpose of allocating payment blocks is to restrict processing of sensitive payment types without subsequent approval. When establishing payment blocks, whether the block can be removed during payment processing or when processing manual payments can be determined. There are two relevant fields;  
  • Change in Payment proposal – if this indicator is set to change (either setting or deleting the block). The block can be changed at the payment proposal stage.  
  • Manual Payment Block – Where the manual payment block has been set, documents which have been blocked cannot be cleared during manual payment entry. |
| Inappropriate access to the automatic payment program | The authorisation objects controlling access to the payment program do not use activity values for access; this often results in the incorrect configuration of access to payment program. |
| Manual cheque payment                   | It is possible to process a manual cheque payment within SAP using the ‘outgoing payment’ functionality. While this function allows the payment to be applied against existing open items, it does not prevent an amount in excess of the existing open items being paid. Access to this function should be strictly controlled. If there is a valid reason to use this function, its use should be subject to close supervision and a manual review should be performed for all manually processed payments. |
| EFT payment run security                | The file used for the electronic payment run is produced from SAP. This file is typically then transferred using bank system EFT systems. Adequate security controls are rarely implemented to minimise the risk of inappropriate changes to the EFT file. |
Significant risks

**High**
- Unauthorised or incorrect EFT payments are processed
- Inappropriate changes are made to payments in the payment program
- Unapproved or incorrect manual payments are made

**Medium**
- Incorrect changes made to recurring payments
- Payment methods are not assigned to vendor accounts

**Segregation of duties risks**
- Vendor Payments / Manual Payments and Purchase Document Approval
- Vendor Payments / Manual Payments and Vendor Maintenance
- Vendor Payments / Manual Payments and Bank Maintenance

Risks and controls

**R227: Unauthorised or incorrect EFT payments are processed**

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Electronic Fund Transfer systems are used to process automatic payments against bank accounts contained in the vendor master record. Inadequate controls operating over these systems can result in fraudulent payments.</td>
</tr>
</tbody>
</table>
| Controls | **Configuration controls**

1. **Adequate security and appropriate controls of EFT files**
   Adequate security of the EFT extract file; and
   Appropriate controls within the EFT system, including dual authorisation processes. (C1036) 

**Manual controls**

1. **Reconciliation controls**
   Reconciliation controls to ensure completeness and accuracy of the extract from SAP to the EFT system. (C268) |
### R228: Inappropriate changes are made to payments in the payment program

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Unauthorised or inappropriate changes are made to payment details during the automatic payment run, resulting in the processing of unauthorised or fraudulent payments.</td>
</tr>
</tbody>
</table>
| Controls | **Configuration controls**  
*Controls to ensure reasonable and complete changes*  
SAP allows changes to be made to documents in the payment proposal run. All changes are only valid within the proposal and do not affect the original documents. Appropriate controls should be implemented to ensure changes performed are reasonable and complete. Fields that are changeable include:  
- Payment (payment method, house bank details, etc.); and  
- Paid items (block indicators, cash discounts, etc.). (C1037) |

### R229: Unapproved or incorrect manual payments are made

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>There is an increased risk in the processing of manual payments; therefore, payments should ideally be processed automatically through SAP.</td>
</tr>
</tbody>
</table>
| Controls | **Manual controls**  
*Obtaining of appropriate authorisation*  
Authorisation in accordance with the entity’s delegation of authority should be obtained before making manual payments. (C267) |

### R230: Incorrect changes made to recurring payments

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Recurring payments may be incorrect resulting in inaccurate payments.</td>
</tr>
</tbody>
</table>
| Controls | **Manual controls**  
*Periodic review of Display Recurring Entry Changes Report*  
A standard report RFAUG0800, transaction code S_ALR_87009883, Display Recurring Entry Changes, listing all changes made to recurring payments should be reviewed periodically to ensure all updates are authorised. (C259) |
R231: Payment methods are not assigned to vendor accounts

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Ideally, payment method should be set to automatic payment for all vendors. Failure to establish a payment method on a vendor could result in the inappropriate processing of a manual payment, potentially resulting in a fraudulent payment.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Controls</th>
<th>Configuration controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Assign appropriate payment methods</td>
</tr>
<tr>
<td></td>
<td>All vendor accounts should be assigned an appropriate payment method. If manual payments are not performed, vendor accounts should not be assigned a manual payment method. (C1038)</td>
</tr>
</tbody>
</table>

Security considerations

Standard payment processing transactions and security objects

<table>
<thead>
<tr>
<th>Security Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td>Description</td>
</tr>
<tr>
<td>FI01, FI02</td>
<td>Create / Change Bank</td>
</tr>
<tr>
<td>FI07</td>
<td>Change Current Number Range Number</td>
</tr>
<tr>
<td>F110, F111</td>
<td>Automatic Payment Program</td>
</tr>
<tr>
<td>FCH5</td>
<td>Manual cheque payments</td>
</tr>
<tr>
<td>F112</td>
<td>Change House Banks/Bank Accounts</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>F_BL_BANK</td>
<td>Authorisation for House Banks and Payment Methods</td>
</tr>
<tr>
<td>F_BNKA_BUK</td>
<td>Banks: Authorisation for Company Codes</td>
</tr>
<tr>
<td>F_REGU_KOA</td>
<td>Automatic payment program by Account Type</td>
</tr>
<tr>
<td>F_REGU_BUK</td>
<td>Automatic payment program by Company Code</td>
</tr>
<tr>
<td>F_BNKA_MAN</td>
<td>Banks: General Maintenance Authorisation</td>
</tr>
<tr>
<td>Entity Values</td>
<td>Bank Code</td>
</tr>
<tr>
<td>BUKRS</td>
<td>Company Code</td>
</tr>
</tbody>
</table>
Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Payments /</td>
<td>Purchase Document</td>
<td>A user may be able to purchase unauthorised goods and releasing a payment to the supplier without further approval of management. This can result in misstating the financial statements arising from misappropriation of the assets.</td>
</tr>
<tr>
<td>Manual Payments</td>
<td>Approval</td>
<td></td>
</tr>
<tr>
<td>Vendor Payments /</td>
<td>Vendor Maintenance</td>
<td>A user could create a ghost vendor or change an existing vendor’s bank account and direct an existing invoice for payment. In addition, a user may create a fictitious vendor or collude with an existing vendor to receive unauthorised discounts and payments resulting in misappropriation of payment funds.</td>
</tr>
<tr>
<td>Manual Payments</td>
<td>Bank Maintenance</td>
<td>A user could create a fictitious bank account and process a payment to it.</td>
</tr>
</tbody>
</table>

Optimising the SAP control environment

- Payment configuration settings
- Maximum payments
- Payment block reasons
- Minimum payments
Better practice procedures which improve the way in which payments are entered for processing completely may include:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
</table>
| Payment configuration settings | Payment processing can be controlled via various configuration settings, including the following:  
  - The system can be configured so that it will always maximise the cash discount available. If this is set, the system will pay invoices early if this results in a payment discount;  
  - Payment methods can be defined, including the default method of payment; and  
  - Minimum payment amounts can be defined per payment methods. |
| Maximum payments            | It is possible to define the maximum amount that can be processed through a bank account via the payment program parameters. If the limit is exceeded, an error message will appear on screen. |
| Payment block reasons       | Payment blocking reasons can be defined for invoices. The following restrictions can be defined:  
  - Whether the block can be set or deleted when processing a payment proposal. This should be prevented for invoice verification payment blocks and payments which have been blocked at the master record level;  
  - Whether documents with a specified blocking flag cannot be cleared with a manual outgoing payment. This should not be possible for any payment block indicator; and  
  - Whether the payment block can be protected from being cancelled online by the user. Note that this restriction can only be applied to one blocking reason and should be activated to prevent invoices blocked during invoice verification (Materials Management module) from being cancelled online. |
| Minimum payments            | Minimum payment values should be set at an appropriate level for each payment media type to assist with implementing cost-effective payment methodologies. |
Chapter 3

General Ledger

3.1 General Ledger Master Maintenance 64
3.2 General Ledger Postings / Reconciliation 71
3.3 New General Ledger 78
IMPORTANT UPDATE
Functional overview

The primary function of the General Ledger is to provide a comprehensive picture for external accounting and accounts. The General Ledger records all business transactions and is fully integrated with all components of SAP, thereby serving as a central reference for all business transactions.

This chapter discusses risks and controls for SAP General Ledger and includes a discussion of risks that entities should consider if implementing the New General Ledger functionality component of ECC 5 / ECC 6.
3.1 General Ledger Master Maintenance

General Ledger master overview

General Ledger account master records contain the data that is always needed by the General Ledger to determine the account’s function. The General Ledger account master records control the posting of accounting transactions.

The General Ledger master data function involves maintaining the Chart of Accounts used in the various company codes. One Chart of Accounts can be used for multiple company codes or a unique Chart of Accounts can be used for each company code.
Commonly identified control weaknesses

The following control weaknesses typically occur in the maintenance of General Ledger master data:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to segregate the ability to maintain General Ledger accounts and process journals.</td>
<td>The ability to maintain General Ledger accounts is often not segregated from the ability to post journal entries. This increases the risk that journals could be processed in unauthorised accounts, potentially impacting on the integrity of the financial statements.</td>
</tr>
<tr>
<td>Posting period authorisation groups</td>
<td>The authorisation group on the posting period control for the General Ledger allows individuals with the proper authorisation to post to accounting periods that might otherwise be closed to others. The authorisation group should be assigned at the end of the posting period to allow authorised finance staff to post period end journals while at the same time restricting access for other staff.</td>
</tr>
</tbody>
</table>

Significant risks

- **High**
  - General Ledger system is inadequately configured
  - Duplicate, incorrect, or unauthorised maintenance of General Ledger accounts

- **Medium**
  - Incorrect maintenance of accounting periods
  - Incorrect maintenance of exchange rates

- **Segregation of duties risks**
  - General Ledger account maintenance and journal processing
  - Maintain Posting Periods and Journal Processing
  - General Ledger account maintenance and Foreign Currency Maintenance
Risks and controls

R300: General Ledger system is inadequately configured

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
</table>
| Risk description | Failure to correctly configure the General Ledger can result in a number of significant business impacts including:
  - Incorrect General Ledger postings impacting on the accuracy of the financial statements.
  - Inaccurate profit and loss and balance sheet reporting.
  - Failure to adequately and accurately interface sub ledger transactions into the General Ledger creating reconciliation problems. |
| Controls | Configuration controls |
| | 1. Set up document type and posting keys (C463/C485/C489) |
| | The posting keys determine which side of an account can be posted to (i.e. a debit or credit transaction) and the type of account that can be posted to (Customer or Vendor account). The correct set up of posting keys is important to ensure appropriate accounting treatment for key transactions. SAP recommends that the standard posting keys are used. |
| | The following posting keys should be reviewed for customer and creditor accounts. |
| | **Customer** | **Vendor** |
| | 01 Invoice – Debit | 21 Credit Memo – Debit |
| | 11 Credit Memo – Credit | 22 Reverse Invoice – Debit |
| | 12 Reverse Invoice – Credit | 25 Outgoing Payment – Debit |
| | 8 Payment Clearing – Credit | 31 Invoice – Credit |
| | Correct set up of fiscal year and accounting periods (C573) |
| | Account groups are correctly assigned to profit and loss accounts (C574) |
| Manual controls | Change management procedures (C1022) |
| | Change management procedures should ensure that changes to General Ledger master data to be documented and appropriately approved. The procedure should cover changes to:
  - Accounting periods
  - Changes to document types
  - Changes to posting keys
  - Changes to the assignment of account groups |
<p>| | Periodic review of account assignment groups (C575) |
| | The account assignment model is critical in ensuring transactions are settled to the correct General Ledger account. |
| | The entity should periodically review changes to the account assignment model to ensure changes have been appropriately approved and implemented. |</p>
<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Inconsistent or incorrect Chart of Accounts is used potentially resulting in incorrect financial statement reporting. Unauthorised changes are made to the chart of accounts.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td>Set key fields for General Ledger master records (C1023)</td>
</tr>
<tr>
<td></td>
<td>Key General Ledger fields should be required for entry and whether the fields should be required or suppressed. It is particularly important that the reconciliation account is a required field for Asset, Material, Vendor and Customer accounts. This will ensure that manual postings cannot be posted in the General Ledger for these accounts.</td>
</tr>
<tr>
<td></td>
<td>Implement general ledger account field settings for security authorisations checks (C630)</td>
</tr>
<tr>
<td></td>
<td>Field group authorizations can be useful to provide additional security control over key General Ledger account fields and is useful for increasing security controls over key General Ledger account fields. Using the authorisation object ‘G/L Account: Account authorisation’ it is possible to restrict the range of General Ledger accounts that a user can maintain. Consideration should be given to using this object.</td>
</tr>
<tr>
<td></td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td>Establish a process for authorisation of new or changes to General Ledger accounts (C387)</td>
</tr>
<tr>
<td></td>
<td>A standard form is typically used to record requests for new or changes to General Ledger accounts. Approval should be obtained from Finance management for the establishment of new accounts and the modification of existing accounts.</td>
</tr>
<tr>
<td></td>
<td>Periodically review changes to General Ledger master records (C807)</td>
</tr>
<tr>
<td></td>
<td>Report Changes to General Ledger master records: RFSABL00 lists all changes to General Ledger accounts. This report should be periodically reviewed to assess the reasonableness of changes.</td>
</tr>
</tbody>
</table>
## R302: Incorrect maintenance of accounting periods

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>When a General Ledger journal or accounting transaction is processed in SAP it must be processed to an accounting period. Ineffective maintenance of posting periods impacts on the integrity of monthly and financial accounts.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td>Posting periods (C811)</td>
<td>SAP provides functionality to set the timeframe for posting periods. An authorisation group can also be specified to minimize the risk of users posting to previous posting periods. The authorisation group on the posting period control for the General Ledger allows individuals with the proper authorisation to post to accounting periods that might otherwise be closed to others. The authorisation group is only typically assigned at the end of the posting period to allow authorised finance staff to post period end journals while at the same time restricting access for other staff. Control Level – Client Security Implications – Access to posting period can be restricted by an authorisation group which is controlled by authorisation object F_BKPF_BUP.</td>
</tr>
</tbody>
</table>

## R303: Incorrect maintenance of exchange rates

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Incorrect exchange rates may be used when processing General Ledger postings, impacting on the integrity of the financial statements. The incorrect maintenance of exchange rates can also result in overpayments of amounts owed in foreign currency.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td>Exchange rate tolerances should be established (C551)</td>
<td>Tolerances for exchange rate differences should be established for company codes and each currency of interest provides the ability to define a maximum difference between exchange rates for posting in foreign currencies. The tolerance defines how much the exchange rate entered manually in the document header may differ in terms of percent from the one stored in the system. If an exchange rate or the local and the foreign currency amount were entered manually during document entry, then a comparison is made with the exchange rates stored in the system. If a deviation occurs and it exceeds the percentage rate specified, a warning message appears.</td>
</tr>
</tbody>
</table>
Security considerations

Key General Ledger master data security considerations include:

- The function of processing General Ledger entries should be appropriately segregated from the functions of maintaining the Chart of Accounts and the financial statements structures, maintaining master records (General Ledger accounts, customer and vendor accounts, asset master records, and bank accounts), and the maintenance of validations and substitutions in the system.

- The ability to open and close posting periods should be restricted to a limited number of finance users only.

Key transaction codes and authorisation objects for the General Ledger

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td>Description</td>
</tr>
<tr>
<td>FS01, FS02</td>
<td>Create General Ledger Account</td>
</tr>
<tr>
<td>FS00</td>
<td>Central General Ledger Account Maintenance</td>
</tr>
<tr>
<td>GP12N</td>
<td>Planning Profile Setup(New GL)</td>
</tr>
<tr>
<td>OB52</td>
<td>Maintain posting periods</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>F_SKAI_BUK</td>
<td>GL Master Record Maintenance by Company Code</td>
</tr>
<tr>
<td>F_SKAI_KTP</td>
<td>GL Master Record Maintenance within Chart of Accounts, by area</td>
</tr>
<tr>
<td>F_SKA1_AEN</td>
<td>Restrict access to sensitive General Ledger fields</td>
</tr>
<tr>
<td>F_BKPF_BES</td>
<td>Restrict accounting postings to sensitive General Ledger accounts.</td>
</tr>
<tr>
<td>F_BKPF_BUP</td>
<td>Accounting Document: Authorisation for Posting Periods</td>
</tr>
</tbody>
</table>
Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Ledger</td>
<td>Journal Processing</td>
<td>Combined access to General Ledger processing, maintenance and master data functions may result in undetected errors and/or irregularities in General Ledger processing. For example, an incorrect General Ledger account could be created to hide inappropriate postings impacting on financial statement integrity.</td>
</tr>
<tr>
<td>account maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain Posting Periods</td>
<td>Journal Processing</td>
<td>Open a previously closed period and post incorrect or fraudulent journals.</td>
</tr>
<tr>
<td>General Ledger</td>
<td>Foreign Currency</td>
<td>Set up an incorrect General Ledger master record and process an inappropriate tax or foreign currency posting.</td>
</tr>
<tr>
<td>account maintenance</td>
<td>Maintenance</td>
<td></td>
</tr>
</tbody>
</table>

Optimising the SAP control environment

- Restricting access to sensitive General Ledger accounts

Better practice items to consider in the use of the General Ledger include:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricting access to sensitive General Ledger accounts</td>
<td>Where there are sensitive General Ledger accounts, authorisation groups can be set on these accounts to restrict access. Access can be restricted through authorisation object F_BKPF_BES.</td>
</tr>
</tbody>
</table>
3.2 General Ledger Postings / Reconciliation

Functional overview

The General Ledger is part of the Financial Accounting module in SAP. General Ledger processing involves the posting of general journals and other periodic postings such as accrual entries. Many transaction postings from other modules (i.e. acquisition of assets, purchases, sales) also result in a real time update of the relevant accounts in the General Ledger.

Commonly identified control weaknesses

The following control weaknesses typically occur in processing General Ledger postings and performing reconciliations:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to segregate the ability to maintain General Ledger accounts and process journals</td>
<td>The ability to maintain General Ledger accounts is often not segregated from the ability to post journal entries. This increases the risk that journals could be processed in unauthorised accounts potentially impacting on the integrity of the financial statements.</td>
</tr>
<tr>
<td>Restricting access to ability to process General Ledger journals</td>
<td>SAP provides a transaction code FB01 which allows finance staff to process Accounts Payable Invoices, Accounts Receivable invoices and General Ledger journals. Often access to this transaction is provided to staff not responsible for processing General Ledger journals, increasing the risk of unauthorised journal processing.</td>
</tr>
</tbody>
</table>

Significant Risks

- **High**
  - Ineffective reconciliation of SAP modules and external interfaces
  - Duplicate or incorrect General Ledger journals
  - Failure to adequately reconcile key bank accounts

- **Medium**
  - Negative postings are permitted
  - Parked journals are not actioned on a timely basis
  - Failure to adequately perform period end procedures

- **Segregation of duties risks**
  - General ledger account maintenance and Journal Processing
  - Maintain Posting Periods and Journal Processing
Risks and controls

R304: Ineffective reconciliation of SAP modules and external interfaces

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Although SAP is an integrated system, reconciliation of key General Ledger accounts is critical and still required. Failure to fully reconcile the General Ledger and external systems increases the risk that the financial statements may be incorrect. Failure to reconcile the Controlling module with the New General Ledger (see page 78 for more information) increases the risk that the financial statements may be incorrect. Vendor, Customer and Assets accounts must be set up as reconciliation accounts to eliminate the risk that direct changes can be made to these accounts through the General Ledger.</td>
</tr>
</tbody>
</table>

Controls

Configuration controls

- **Reconciliation ledger capability (C717)**
  One of the inherent limitations of the traditional General Ledger (see page 78 for more information on the difference between New General Ledger and the traditional General Ledger) are issues with reconciliation between the Financial Accounting (FI) and Controlling (CO) modules. SAP provides a reconciliation ledger capability to assist with the reconciliation process.

- **Reconciliation accounts (C564)**
  Accounts Payable, Customer and Asset accounts should be set up as reconciliation accounts to restrict the ability to process manual journals to these accounts.

Manual controls

- **Regular review of reports that assist in reconciling the General Ledger to SAP sub-ledgers (C477)**
  SAP provides two reports which assists in reconciling the General Ledger to SAP sub-ledgers. Report SAPFO70 Reconcile documents and Accounts transaction figures, compares document and account transaction figures. Report SAPF190 Financial Accounting Comparative Analysis, compares debit and credit transactions of Customer, Vendor and General Ledger accounts against the debit and credit totals of posted documents. Both of these reports should be reviewed on a regular basis.

- **Reconciliation of all external interfaces (C397)**
  All external interfaces should be regularly reconciled. Interface error reports should be regularly reviewed and actioned. All interface errors must be followed up to ensure the integrity of the financial statements.
## R305: Duplicate or incorrect General Ledger journals

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
</table>
| Risk description | The processing of incorrect or unauthorised General Ledger journal postings can result in manipulation of financial results impacting on the integrity of the financial statements. Key risks include:  
- duplicate journal entries are processed;  
- unauthorised journals are processed to manipulate financial results; and  
- journals are processed to the wrong General Ledger account or for the wrong amount. |

### Controls

#### Configuration controls

**Park and post approval controls**

Park and post automated workflow approval should be established for the automated approval of General Ledger journals. (C555)

If automated park and post approval processes are not being used, it is important that all journals entries are appropriately authorised according to the entity’s delegations of authorities. (C392)

**Set posting tolerances (C552)**

It is possible to set posting tolerances for individual users or for user groups. This control relates to the allocation of users to individual tolerances.

**Restrict the ability to change key fields (C386)**

Document change rules define under which circumstances fields can be changed after posting. SAP restricts the ability to change key fields required for the integrity of the system including the amount, account, business area and cost centre. However, other fields can be modified. It is important to restrict the ability to change key fields to ensure transaction integrity and maintain an effective audit trail.

**Validations (C385)**

Validations are used to implement entity or business specific internal control requirements, such as restricting the ability to post to sensitive accounts. It is possible to establish validations on both the document header and individual document items. Validations can be set for both manual entry and automatic document creation.
## R305: Duplicate or incorrect General Ledger journals (continued)

<table>
<thead>
<tr>
<th><strong>Manual controls</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Review of The Compact Journal Report (C396)</td>
</tr>
<tr>
<td>The Compact Journal Report (RFBELJ00) should be reviewed to identify potential duplicate and incorrect journal entries.</td>
</tr>
<tr>
<td>Periodic review of Recurring Entry Documents Report (C395)</td>
</tr>
<tr>
<td>It is important to periodically review recurring journals via report RFDAUB00, transaction code S_ALR_87009883 Recurring Entry Documents.</td>
</tr>
<tr>
<td>Correct set up of posting keys (C463)</td>
</tr>
<tr>
<td>The correct set up of posting keys is important to ensure appropriate accounting treatment for key transactions. The posting keys determine which side of an account can be posted to (i.e. be it a debit or credit transaction) and the type of account that can be posted to (Customer or Vendor account).</td>
</tr>
</tbody>
</table>

## R306: Failure to adequately reconcile key bank accounts

<table>
<thead>
<tr>
<th><strong>Risk rating</strong></th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk description</strong></td>
<td>Failure to adequately reconcile bank accounts impacts on the integrity of the financial statements and cash flow position.</td>
</tr>
<tr>
<td><strong>Controls</strong></td>
<td>Manual controls</td>
</tr>
<tr>
<td>Periodic reconciliation of all bank accounts (C567)</td>
<td></td>
</tr>
<tr>
<td>Periodic reconciliation of all bank accounts must be performed. All reconciling items should be adequately followed up and actioned.</td>
<td></td>
</tr>
</tbody>
</table>

## R307: Negative postings are permitted

<table>
<thead>
<tr>
<th><strong>Risk rating</strong></th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk description</strong></td>
<td>Incorrect negative postings may result in incorrect General Ledger postings possibly impacting on the accuracy of the financial statements.</td>
</tr>
<tr>
<td><strong>Controls</strong></td>
<td>Configuration controls</td>
</tr>
<tr>
<td>Specify whether negative postings are permitted (C483)</td>
<td></td>
</tr>
<tr>
<td>It is possible to specify by company code whether reversal documents can contain negative postings. When reversing transactions, it is possible to either reverse the original transaction or make a negative posting. Reversing the original transaction is preferred from an internal control perspective.</td>
<td></td>
</tr>
</tbody>
</table>
### R308: Parked journals are not actioned on a timely basis

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>The park functionality is often used to enter journals that have outstanding items or questions. There is a risk that parked journals entered into SAP are not subsequently actioned.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td><em>Periodic checks to identify held or parked documents (C1039)</em> On a periodic basis (i.e. monthly) a check should be performed to identify any documents that are ‘held’ or ‘parked’ within the system to ensure that all documents are processed in the correct accounting period.</td>
</tr>
</tbody>
</table>

### R309: Failure to adequately perform period end procedures

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Incorrect or incomplete performance of period end procedures can result in the processing of inappropriate period end transactions or the failure to perform key period end procedures including reconciliation of key accounts.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td><em>Period end procedures outlining key reconciliation procedures (C1021)</em> Period end procedures outlining key reconciliation procedures should be developed and followed at period end.</td>
</tr>
<tr>
<td></td>
<td><em>Reports that can assist to adequately perform period end closing process (C872)</em> There are a number of useful SAP reports that can assist in the performance of an adequate period end closing process. These reports include:</td>
</tr>
<tr>
<td></td>
<td>• S_PLO_86000030 − Account balance report</td>
</tr>
<tr>
<td></td>
<td>• S_ALR_870122777 − Review balances, debit and credit amounts for the period.</td>
</tr>
</tbody>
</table>
Security considerations

Key General Ledger security considerations include:

- Consideration should be given to restricting access to financial accounting transactions by company code, business area, document type and account type. Users can be restricted to post to only General Ledger accounts, for example using the authorisation object ‘Accounting document: Authorisation for account types’.

- Access to the transactions required to create a recurring entry reference document and to run the recurring entry posting program should be restricted to a limited number of users.

Key transaction codes and authorisation objects for the General Ledger

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td>Description</td>
</tr>
<tr>
<td>FB01</td>
<td>General Ledger posting</td>
</tr>
<tr>
<td>GP12N</td>
<td>Planning Profile Setup(New GL)</td>
</tr>
<tr>
<td>FBL1N</td>
<td>Vendor Line Item Display</td>
</tr>
<tr>
<td>FBL6N</td>
<td>Customer Line Item Display</td>
</tr>
<tr>
<td>FB50</td>
<td>General Ledger Account Posting</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>F_BKPF_BUK</td>
<td>Accounting Document by Company Code</td>
</tr>
<tr>
<td>F_BKPF_KOA</td>
<td>Accounting Document by Account Type</td>
</tr>
</tbody>
</table>

Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Ledger account maintenance</td>
<td>Journal Processing</td>
<td>Combined access to General Ledger processing, maintenance and master data functions may result in undetected errors and/or irregularities in general ledger processing. This can result in misstatement in the financial statements. For example, an incorrect General Ledger account could be created to hide inappropriate postings impacting on financial statement integrity.</td>
</tr>
<tr>
<td>Maintain Posting Periods</td>
<td>Journal Processing</td>
<td>Open a previously closed period and post an incorrect or fraudulent journal transaction.</td>
</tr>
</tbody>
</table>
Optimising the SAP control environment

Better practice items to consider in the use of General Ledger component include:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
</table>
| General Ledger posting tolerances | Limits can be defined to limit the amounts that users can post General Ledger journals for, including:  
  - the maximum amount that the user can post in any one document;  
  - the maximum amount that the user can enter in a single line item for a vendor/customer account;  
  - the maximum percentage cash discount that the user can enter per line item in a document; and  
  - the limit up to which payment differences are permitted. |
| Segregating the ability to park and post journals | Authorisation of General Ledger journals is a critical risk within the General Ledger process. Park and post workflow functionality can be implemented to enable automated approval of journals.  
If implementing the full park and post functionality is too difficult, another option is to allocate the park and post security transactions to separate users. |
3.3 New General Ledger

Functional overview

Within ECC5 / ECC6, a New General Ledger component has been introduced. When implementing ECC5 or ECC6, entities can choose to either use the traditional General Ledger component or to implement the New General Ledger.

New General Ledger provides many benefits from an audit and control perspective including:

- **Improved reporting**: Management reporting is improved through enhanced segment and company code reporting.
- **Integration**: Where the traditional General Ledger requires the reconciliation of multiple applications, New General Ledger provides an integrated structure that includes the functions: cost of sales ledger, profit centre accounting, special ledger, and the consolidation staging ledger. A benefit of this is that, when appropriately configured, it reduces the end of period reconciliation between the Controlling and General Ledger components.
- **Fast close**: Improves transparency for auditing and corporate governance purposes. In addition, it accelerates period-end.
Commonly identified control weaknesses

The following control weaknesses typically occur in New General Ledger implementations:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master data integrity concerns as a result of inappropriate configuration of the New General Ledger</td>
<td>The integrity of New General Ledger reports depends on whether master data items, including cost centre and profit centre records, have been assigned an appropriate segment record. Often these master data items have integrity problems resulting in incorrect segment reporting from the New General Ledger.</td>
</tr>
</tbody>
</table>

Significant risks

- New General Ledger is inadequately configured

Risks and controls

**R310: New General Ledger is inadequately configured**

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>The New General Ledger component facilitates the reporting of segment and profit centre reporting. This component must be configured correctly to allow effective reporting. Key New General Ledger risks include:</td>
</tr>
<tr>
<td></td>
<td>• Document splitting for New General Ledger functionality is configured inappropriately and not functioning in line with business requirements.</td>
</tr>
<tr>
<td></td>
<td>• Inaccurate management and segment reporting.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td>Activating New General Ledger</td>
</tr>
<tr>
<td></td>
<td>To use the New General Ledger it must be activated within the SAP configuration. Assess whether the New General Ledger has been activated. Activating the New General Ledger enables the New General Ledger IMG path. (C914)</td>
</tr>
<tr>
<td></td>
<td>Zero balancing</td>
</tr>
<tr>
<td></td>
<td>If New General Ledger reporting is used, effective zero balancing must be configured for key reporting criteria. Where zero balancing is enabled, and a profit centre is not allocated a segment or a cost centre is not allocated a profit centre, SAP is able to determine whether to post the New General Ledger item. (C918)</td>
</tr>
<tr>
<td></td>
<td>Activation of document splitting</td>
</tr>
<tr>
<td></td>
<td>Document splitting should be activated for each company code. Advanced document splitting rules must be enabled to determine applicable segments to post entries. (C921) (C928)</td>
</tr>
</tbody>
</table>
Security considerations

There are no significant impacts on security from the introduction of the New General Ledger component. The New General Ledger does provide the ability to set up multiple ledger groups. Transaction FB50L has been introduced to enter posting to different ledgers.

Key transaction codes and authorisation objects for the General Ledger

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FB50L</td>
<td>General Ledger Account Posting (New General Ledger)</td>
</tr>
</tbody>
</table>

Optimising the SAP control environment

- Review integrity of master data
- Ability to maintain the traditional and New General Ledgers to enable reconciliation
- Set up advanced document splitting rules

Better practice items to consider in the use of the New General Ledger component include:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review integrity of master data</td>
<td>To enable accurate segment reporting, all profit centres must be allocated a segment record and cost centres must be allocated a profit centre. Before implementing New General Ledger it is important to review and improve the integrity of cost and profit centre records.</td>
</tr>
<tr>
<td>Ability to maintain the traditional and New General Ledgers to enable reconciliation</td>
<td>It is possible to configure SAP to update both the traditional and New General Ledger. This may be useful in the initial stages of the implementation of the New General Ledger. After the implementation is complete, to minimise any performance implications, it is best to turn this functionality off.</td>
</tr>
<tr>
<td>Set up advanced document splitting rules</td>
<td>Where two expense items with different segments as an example are posted in the same document, it is difficult for SAP to determine which segment to post to. To address this issue, each document type is allocated a business transaction and variant which is then assigned an enhanced document splitting rule. The rule looks at each item in the transaction to determine where to inherit the segment from.</td>
</tr>
</tbody>
</table>
Chapter 3 – Feature article

Shared Services

Overview
Significant risks
Security considerations
Overview

Shared Services environments are being implemented using SAP within both the public and private sectors. The rationale for creating shared services environments is the reduction in both infrastructure and ongoing maintenance costs.

In the past few years a number of public sector entities have consolidated the number of SAP instances that they run and implemented a shared services environment which lowers IT spending, particularly on the number of servers required and reduced support costs.

Implementation of shared services may facilitate improvements and efficiencies in management of IT infrastructure; however, it often results in increased interdependencies and complexities between infrastructure and applications which may create new security and control risks.

This chapter of the guide outlines risk areas to consider when considering the use of Shared Services.

Significant risks

In addition to the risks identified for other SAP components, the implementation of shared services creates several additional risks which require consideration during the implementation process. These additional risks require controls and ongoing monitoring as a part of normal, business as usual activities. The following implementation considerations should also be considered. They are further described in the Impacts and controls table.

Chapter 5: Basis – Monitoring for cross-talk

- Implementing consistent and effective business processes in the control environment
- Assigning responsibility for key elements of the control environment
- Segregating and restricting access across organisational areas
What are the key tasks that assist in the implementation of an effective SAP security and control environment for the implementation of Shared Services?

Implementation of shared services often involves consolidating a number of separate SAP instances into one. Generally, each of the separate ‘legacy’ instances and business entities are very different, and these differences extend to differences in business processes and controls.

A key risk in these projects is ensuring that sufficient attention is provided to the implementation of adequacy, security, configuration and process controls.

The following outlines the tasks that were performed in each phase of the implementation.

- **Prepare Project Plan**
  - Identify key tasks required to embed adequate security and control and ensure that these tasks are included in the project.
  - For example:
    - Review project plan to understand project milestones and control checkpoints
    - Assess the process for documenting key controls. Determine the education process to educate project team members of the importance of security and control implementation
    - Conduct project risk assessment
    - Review project risk management process

- **Develop Configuration Control Guide**
  - Develop Configuration Control Guides that outline key configuration controls. These are also known as ‘risk and control matrices’ and document key controls that are important for business processes.
  - In addition, depending on the complexity of business processes, segregation of duties rules are either identified in the control guide or separately in ‘access control matrices’.
  - These documents should be distributed to the project team and key business stakeholders.

- **Implement solution**
  - The configuration of the SAP system is reviewed to identify whether applicable configuration controls had been adequately implemented. Security roles were reviewed for segregation of duties conflicts.

- **Test and accept solution**
  - All changes to configuration controls and security roles resulting from testing are reviewed and their impact on the security and control environment is assessed.

- **Go Live and Post implementation support**
  - Perform a post implementation assessment of key controls and segregation of duties. Assessment may include:
    - Confirmation segregation of duties is effective and assignment of critical functions to roles is appropriate.
    - Determine that the configuration controls implemented are appropriate and effective. This may be achieved using internal audit, or an independent external reviewer for example.
    - Assess the adequacy of operation of manual controls that were implemented to mitigate identified risks.
Security considerations

There are a number of key security risks associated with the implementation of Shared Services including:

Restrict access to critical functions or ‘across-organisation’ (company codes)

Given Shared Services projects result in the implementation of multiple separate organisations or government entities being included within the one SAP instance, completing a critical access risk assessment across organisation elements is important.

Within SAP, each entity has a distinct set of organisational parameters defined for it, including company codes, plant, sales and purchasing organisations and personnel areas. Access to each of these organisation parameters can be restricted through various SAP security authorisation objects.

Within Shared Services entities, access is typically restricted by company code, business area, plant location or personnel area within the payroll process.

It is very difficult to implement effective security that restricts access across organisation levels. Even though user access may be restricted to a specific area such as company code (through the security role or profile configuration), users often get access to other company codes through another security role.

Periodic reporting of the adequacy of access to sensitive organisation splits must be performed to mitigate this risk.

Review and maintenance of SAP security roles

The implementation of Shared Services and consolidation of SAP instances typically often results in an increased number of users and security roles within the SAP system. To effectively manage and review the security risks associated with these users and roles, it is important to correctly classify ownership and responsibility for managing each user account and security role.

User classification is typically performed through the user group field contained within each user master record. For example, all Accounts Payable users are typically assigned to the Accounts Payable user group. The Accounts Payable manager can then be allocated to manage security risks associated with these users. If organisational structures are complex, the use of user group classifications should be considered.

Classification for security roles is more difficult. SAP does not contain a user group type field for the classification of security roles. Entities typically use the role description and an effective role naming structure to assign responsibility for each security role.

Assign responsibility for ongoing monitoring of segregation of duties and critical access

The implementation of Shared Services results in an additional party and set of users being given responsibility for an element of the SAP system.

Responsibilities for detecting and reporting security risks must be allocated to the Shared Services unit. The business area should ensure that periodic reviews of user access and reviews of the appropriateness of roles are performed. Such reviews are important to ensure that access roles continue to enforce business requirements for management of security risks.
## Impacts and controls

<table>
<thead>
<tr>
<th>Objective</th>
<th>Recommended Better Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that the control environment maintains effective configuration and process controls that address organisational risks.</td>
<td>Implementing Shared Services typically results in either the reimplementation of SAP into a new instance or the use of one existing SAP instance. This impacts on the security and control environment, given that a number of different entities and business models are typically consolidated into one SAP instance, which will result in changes to the control environment.</td>
</tr>
<tr>
<td>Assign responsibility for key elements of the control environment</td>
<td>Shared Services increases the complexity for determining monitoring and ongoing maintenance of the control environment. Taking the Accounts Payable process for example, the responsibility for initiating and approving purchases is the responsibility of users, whereas Shared Services is typically responsible for maintaining vendor records and processing invoices. To enable an effective control environment, it is important that responsibility is well-defined between Shared Services and user areas for key controls and security within each area of responsibility.</td>
</tr>
<tr>
<td>Segregate and restrict access across organisational areas and ensure that segregation of duties rules are maintained.</td>
<td>Given Shared Services projects result in the implementation of multiple separate organisations or government entities being included within the one SAP instance, critical access risk assessment across organisation elements is important. For example, it is important that users in the one organisation area do not have access to another organisation’s data. During the implementation process it is important that the risk and importance of segregating access across organisation area is assessed. An effective security structure and monitoring process must be implemented to address organisation access risk.</td>
</tr>
<tr>
<td>Security risks are identified and are addressed.</td>
<td>Review the security risks identified in this chapter. Project assessments should consider the following: • Restrict access to critical functions or across organisational areas; • Classify security roles; and • Review security administration procedures as a PART of the project (and not left until post-implementation). Australian government entities should comply with the Information Security Manual. Project implementations should identify impacts to existing policy/procedural documents and identify timeframes and stakeholders to ensure that such documents are upgraded.</td>
</tr>
</tbody>
</table>
Overview

The main components of the SAP HR module are:

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
</table>
| Personnel Management            | Prior to version 4.6, personnel management was split into two sub-modules known as Personnel Administration and Personnel Planning and Development. These modules were combined in version 4.6 and are now collectively known as Personnel Management. The Personnel Management module is used for:  
  - Maintaining all employee and organisational master data;  
  - Processing employee hiring and termination;  
  - Performing organisational planning, budgeting, and recruitment; and  
  - Administering salaries, benefits, and expenses. |
| Personal Time Management        | This module is used in the planning, recording and valuation of employee work performed and absence times.                                                                                                  |
| Payroll Accounting              | This module provides a number of work processes including the generation of payroll results and remuneration statements, bank transfers and cheque payments.                                                    |
| Employee Self Service (ESS)     | The self service module allows employees to maintain their time sheet, leave requests, personal information, and display of pay slips.                                                                         |
| Managers Desktop                | This module allows functional managers to perform administrative tasks within their area and access relevant HR, financial, or controlling data.                                                             |
4.1 Personnel Management

Functional overview

The Personnel Management module is used for the maintenance of employee standing data, processing hiring/terminations of employees, benefits and payroll, and organisational planning. This is the most significant area of risk in the SAP HR module.

The SAP HR system operates with sets of data records, called infotypes, which each hold specific types of organisational and employee data. Users select an infotype for viewing or updating particular data. Therefore, security in the system is heavily reliant on the infotypes and the associated actions assigned to end users.

Commonly identified control weaknesses

Typical control weaknesses that may occur in the Personnel Management process include:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee master record integrity concerns</td>
<td>The appropriateness of payroll payments depends on the integrity of employee master records. Duplicate employee records often result in duplicate payments. Screen modification rules should be defined to ensure that all key fields are mandatory for data input.</td>
</tr>
<tr>
<td>Infotype logging</td>
<td>Entities do not typically log changes to sensitive infotype records. The Logged Changes in Infotype audit report is useful in identifying inappropriate changes to infotype records.</td>
</tr>
<tr>
<td>Access to sensitive payroll and employee data</td>
<td>The HR system contains sensitive employee records including bank accounts, address details and tax file numbers. Access to this data, either through the front end or through database browsing, is often not secure.</td>
</tr>
<tr>
<td>Use of position base security</td>
<td>For entities utilising SAP HR, position based security, where SAP security roles are assigned to a position within the entity rather than directly to a user master record, should be considered. Users are then assigned to a position when hired into the entity. This provides an improved level of control when users leave the entity or transfer to a different position.</td>
</tr>
</tbody>
</table>
Significant risks

High

- Employee master integrity concerns / employee cost allocations are incorrect
- Employees are not inactivated when employment is terminated
- Unauthorised changes to employee positions and appointments
- Users are able to view sensitive employee data

Segregation of duties risks

- Employee Maintenance and Payroll Processing
- Employee Maintenance and Position Management
- Employee Maintenance – Bank Account and Employee Maintenance – Payroll Status

Risks and controls

<table>
<thead>
<tr>
<th>R400: Employee master integrity concerns / employee cost allocations are incorrect</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk rating</strong></td>
<td><strong>HIGH</strong></td>
</tr>
<tr>
<td><strong>Risk description</strong></td>
<td>Employee details may be incorrectly entered or maintained. This may result in a number of issues, including incorrect cost allocations, duplicate payments, problems with superannuation contribution and employee deductions or the allocation of inappropriate security roles. Duplicate employees may exist on the payroll, resulting in duplicate payments.</td>
</tr>
<tr>
<td><strong>Controls</strong></td>
<td><strong>Configuration controls</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Defining of key data entry fields (C1052)</strong></td>
</tr>
<tr>
<td></td>
<td>Key data entry fields should be defined as ‘required entry’ in the system to ensure that all information necessary to the completion of HR master data is entered. Field settings are able to be controlled for both screen headers and the detailed section of the screen. The standard system settings are defaulted but should be reviewed to ensure that appropriate settings are defined for each entity.</td>
</tr>
<tr>
<td></td>
<td><strong>Manual controls</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Review of new employee details (C1053)</strong></td>
</tr>
<tr>
<td></td>
<td>A subsequent review of new employee details should be conducted by a HR supervisor. Given the importance of the creation of new employees, review of the details in the system is critical to maintaining data integrity.</td>
</tr>
<tr>
<td></td>
<td><strong>Review and actioning of Infotype Audit Report (C621)</strong></td>
</tr>
<tr>
<td></td>
<td>The Infotype Audit Report (RPUAUD00) is a critical control report within SAP Personnel Management. It is configurable and may be used to review changes to key payroll records. The report should be reviewed and actioned every pay period.</td>
</tr>
<tr>
<td></td>
<td><strong>Review of current employees (C1054)</strong></td>
</tr>
<tr>
<td></td>
<td>Procedures should be put in place to ensure that a review of current employees in the system is conducted prior to entering new employees. This will help to mitigate the risk of duplicate employees entered in the system.</td>
</tr>
</tbody>
</table>
### Periodic assessment for employees who are paid as vendors

An entity was concerned that its employees were also providing services and were being paid as vendors. One area of concern was that managers, who were responsible for approving payments, were also approving payments for themselves.

To address this risk, a comparison of employee bank accounts and address records against vendor records was performed. This analysis identified a number of employees who had been paid as vendors. After this analysis, the policy of employees providing services had to be reviewed.

One area that had to be excluded from the analysis was employees who are paid expenses through the Accounts Payable system.

Source: Protiviti Australia

### R401: Employees are not inactivated when employment is terminated.

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Employee records for employees who have left may not be flagged as terminated which may result in subsequent payment or payments to these employees. For entities using ‘single sign on’, failure to inactivate terminated employees may also fail to inactivate network access.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>Employee end dates (C299)</strong></td>
</tr>
<tr>
<td></td>
<td>An end date should be entered against terminated employees (including contractors and non-ongoing employees, if applicable).</td>
</tr>
<tr>
<td></td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td><strong>Notification of termination of employment to the payroll/human resources area (C305)</strong></td>
</tr>
<tr>
<td></td>
<td>HR should be notified by the relevant manager when an employee leaves the entity. A termination form (or exit checklist/form) should be completed, approved by the business unit manager and forwarded to the HR department.</td>
</tr>
<tr>
<td></td>
<td><strong>Review of payroll reports (C587)</strong></td>
</tr>
<tr>
<td></td>
<td>Payroll staff should review payroll reports to ensure terminated employees are not paid in subsequent payroll periods after leaving the entity.</td>
</tr>
<tr>
<td></td>
<td><strong>Approval of employee terminations and associated payments (C586)</strong></td>
</tr>
<tr>
<td></td>
<td>Employee terminations and associated payments should be approved by both the employee’s and the HR manager. HR staff should also review payroll run reports and payroll change reports to ensure that terminated employees are not paid in subsequent payroll periods after the employee has left the entity.</td>
</tr>
</tbody>
</table>
**R402: Unauthorised changes to employee positions and appointments**

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Inappropriate or unauthorised changes are made to the entity / position structure, including salaries and security requirements.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
</tbody>
</table>

**Review Infotype Audit Report (C290)**

The **Infotype Audit Report (RPUAUD00)** is a critical control report within SAP Personnel Management. It is configurable and may be used to review changes to key payroll records. The following three tables must be maintained to allow the report to function:

- T585A – Infotypes to log;
- T585B – Field group definition; and
- T585C – Field group characteristics.

Infotype records in these tables are established based on transaction class. Transaction class **A** relates to HR master records, while transaction class **B** relates to applicants data. The audit report should be reviewed, at least once each pay period.

**Documenting and approving appointments (C1055)**

All appointments should be documented on a standard employee appointment form and be appropriately authorised before the employee is created.

---

**R403: Users are able to view sensitive employee data**

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Unauthorised users may have access to view/maintain sensitive HR/payroll data. This may compromise the confidentiality of HR data and may also result in the processing of fraudulent payroll payments. Access to employee maintenance and display transactions must be restricted.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
</tbody>
</table>

**Restricted access to employee maintenance and display transactions (C1056)**

Access to employee maintenance and display transactions should be restricted to appropriate personnel.

**Restricted data browsing access to payroll tables (C1057)**

SE16 and other data browsing access to payroll tables should be restricted using authorisation object S_TABU_DIS.

**Structural authorisations (C1058)**

Structural authorisations are used in coordination with traditional SAP security authorisations to control access to the SAP HR module. **PD authority profiles** define which objects in the organisational plan a user is permitted to access (i.e. organisational units). HR security roles and authorisations should be given extensive scrutiny during development and should be only assigned on a need basis.
Security considerations

Standard HR Personnel Management security objects that should be restricted to appropriate staff

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td></td>
</tr>
<tr>
<td>PA10</td>
<td>Personnel File</td>
</tr>
<tr>
<td>PA20</td>
<td>Display HR Master Data</td>
</tr>
<tr>
<td>PA30</td>
<td>Maintain HR Master Data</td>
</tr>
<tr>
<td>PA40</td>
<td>Personnel Actions</td>
</tr>
<tr>
<td>HRBEN0001</td>
<td>Benefits Enrolment</td>
</tr>
<tr>
<td>HRCMP0001C</td>
<td>Compensation adjustment change – Salary Review</td>
</tr>
<tr>
<td>HRCMP0060C</td>
<td>Granting Employee Awards: Change</td>
</tr>
<tr>
<td>SE16</td>
<td>Data browsing is used to view employee and payroll information.</td>
</tr>
</tbody>
</table>

Authorisation Objects

<table>
<thead>
<tr>
<th>P_TCODE</th>
<th>HR: Transaction Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>P_ORGIN</td>
<td>HR: Master Data</td>
</tr>
<tr>
<td>P_PERNR</td>
<td>HR: Master Data – Personnel Number Check</td>
</tr>
<tr>
<td>P_ORGXX</td>
<td>HR: Master Data – Extended Check</td>
</tr>
<tr>
<td>S_TABU_DIS</td>
<td>Use to restrict access to sensitive payroll and employee database tables.</td>
</tr>
</tbody>
</table>
• Access to HR master data is provided through information types called ‘infotypes’. Access should be adequately restricted using object HR: Master data (P_ORIGIN).

• The P_ORIGIN authorisation object is used to implement a release process for HR master data. One user may be assigned the ability to create ‘locked’ HR master data records and a second user is then assigned the authority to ‘unlock’ those records.

• It is vital that access to direct table maintenance transactions is restricted appropriately in the system. Users with access to display/maintain tables may also be able to access sensitive HR data.

Chapter 5: Basis

• Personnel officers and payroll staff should be restricted from maintaining their own HR data including basic pay information. This is achieved by:
  - Activating authorisation object HR: Master data – personnel number check (P_PERNR). Based on personnel numbers it is possible to assign particular users the ability to maintain specific personnel numbers; or
  - Activating authorisation object HR: Master data extended check (P_ORGXX). Users can be restricted to maintaining HR master data for a specific group of employees by defining administrators and assigning employees to them. This can effectively be used to segregate HR master data maintenance. The personnel number check must also be activated in the system; or
  - Restricting the access of payroll staff to perform only payroll functions while HR staff maintains only employee standing data.

• PD authority profiles should be created to limit an employee’s access to specific personnel planning and development objects or organisational structures, and to control the activities that users perform for organisational plans. These profiles built on an access limiting basis, therefore, if a user is not allocated a PD authority profile, they would have access to all organisational objects.

• Structural authorisations. Structural authorisations are used to restrict access to elements of the entity structure. For example, a manager’s access in payroll security is able to be restricted to the employee that the manager is responsible for.
### Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Maintenance</td>
<td>Payroll Processing</td>
<td>HR functions including master data maintenance, the commencement/termination of employees, salary administration and maintaining leave balances should be segregated from the payroll processing function. Combining these duties significantly increases the risk of fraudulent activity.</td>
</tr>
<tr>
<td>Employee Maintenance</td>
<td>Position Management</td>
<td>A user could alter an employee’s position and bank account details to allow a fraudulent payment. Altering the position to a higher position, could result in a significant overpayment.</td>
</tr>
<tr>
<td>Employee Maintenance – Bank Account</td>
<td>Employee Maintenance – Payroll Status</td>
<td>A user could change the status of an expired employee and change the bank account of that employee to their own. The employee would then be paid in the pay run and the payment would go to the user.</td>
</tr>
</tbody>
</table>

### Optimising the SAP control environment

- Delimit data
- Sensitive employee groups
- HR events
- Employee data integrity analysis
- Data release
- Payroll status
- Termination procedures
## IMPORTANT UPDATE

**Human Resources**

### Area Description

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delimit data</td>
<td>Procedural controls should be in place to ensure that changes made to infotypes for HR master data are performed by delimiting or creating a new infotype with new validity dates. This provides an audit trail of all change activity on the HR master record and helps to ensure that all records required for statutory purposes are retained.</td>
</tr>
<tr>
<td>Sensitive employee groups</td>
<td>A senior administrator should be designated for maintaining particular types of data for sensitive personnel groups (i.e. senior executives of the entity). This may be prudent to protect the entity from internal or external scrutiny.</td>
</tr>
<tr>
<td>HR events</td>
<td>Different types of employee master data is able to be grouped together to create 'events'. Events are used to control the information that will be processed when commencing, terminating, and maintaining employee data. Groups of master data should be appropriately configured to ensure that all relevant information is entered during the predefined events processed in the HR module.</td>
</tr>
<tr>
<td>Employee data integrity analysis</td>
<td>Regular analysis of the integrity of employee data should be assessed. Typical areas to review include the identification of duplicate employees, employee integrity issues such as employees with unallocated cost centres, and matching vendor and employee details.</td>
</tr>
<tr>
<td>Data release</td>
<td>The ‘double verification principle’ should be considered to ensure that master data changes are completely processed. One user is assigned the ability to create ‘locked’ HR master data records. A second user is then assigned the authority to ‘unlock’ those records after performing a check and online authorisation of the first user’s activities.</td>
</tr>
<tr>
<td>Payroll status</td>
<td>Access to the payroll status record (which determines whether a user is included in the payroll) should be restricted and any changes logged for review by management. It is possible to change the status of a terminated user to enable payment, even after termination.</td>
</tr>
</tbody>
</table>
| Termination procedures        | Procedures should be developed to ensure that any master data (infotype) that is not automatically deactivated as part of the ‘termination’ event is deactivated as part of the termination processing.  
Procedures should be developed to ensure that users retain this data on the system for future reference and processing of any subsequent payments.  
A standard checklist should be developed as part of termination procedures to ensure that all relevant master data settings are deactivated after termination.  
However, there are some master data elements that should not be deactivated even after an employee has been terminated. This includes organisational data, personal data, address data and basic pay data. |
4.2 Personal Time Management

Personal Time Management provides processes supporting the planning and recording of employee work hours. A significant change in Personal Time Management is Cross Application Timesheet (CAT) functionality that provides a standard interface for recording time across components of SAP. CAT combines existing SAP time recording functions into a single process and provides information to other components including:

- internal activity allocation for Controlling; and
- Personal Time Management for attendances and absences.

Commonly identified control weaknesses

Control weaknesses that occur in the Personal time management module include:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy of employee time data</td>
<td>Employee payments, particularly for contract and casual employees, rely on the accuracy of timesheet data. Field selections should be configured as required input, display, hidden or highlighted in the user screens are often not configured, thus impacting the integrity of timesheet data.</td>
</tr>
<tr>
<td>Incorrect classification of overtime hours or calculation of flex leave</td>
<td>Overtime compensation types and wage types, such as flexleave should be appropriately defined to ensure that, where overtime is entered, it is accurately accounted for.</td>
</tr>
</tbody>
</table>

Significant risks

- Medium
  - Inaccurate or untimely entry of timesheet data

- Segregation of duties risk
  - Timesheet Entry and Timesheet Approval
  - Timesheet Assessment and Process Payroll
## Risks and controls

### R404: Inaccurate or untimely entry of timesheet data

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Timesheet data is inaccurately entered in the system, resulting in incorrect payments to employees or inaccurate accounting of employee leave.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td>Automated notifications (C1059)</td>
</tr>
<tr>
<td></td>
<td>On days when time reporting is due, automated notifications should be configured to remind users to enter their time report.</td>
</tr>
<tr>
<td></td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td>Timesheet approval and review (C1060)</td>
</tr>
<tr>
<td></td>
<td>All timesheets should be approved by a functional manager and reviewed against a master work schedule. Any discrepancies should be followed up or the report rejected. Rejection reasons should be configured to give employees an understanding of the issue and a solution for rectifying the situation.</td>
</tr>
<tr>
<td></td>
<td>Use, approval and lodging of standard leave forms (C335)</td>
</tr>
<tr>
<td></td>
<td>For accurate accounting of employee leave, a standard leave form should be used to record employees’ requests for leave. All leave requests should be appropriately approved by the employee and the employee’s immediate supervisor. The leave form should be lodged with the scheduling manager.</td>
</tr>
</tbody>
</table>
Security considerations

Access should be restricted to the following Personal Time Management sensitive transactions; approval of time sheets should be restricted to relevant functional managers and/or HR staff:

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAT2, CAT3</td>
<td>Time Sheet: Initial Screen</td>
</tr>
<tr>
<td>CAPS</td>
<td>Time Sheet: Approve Times (Select by Master Data)</td>
</tr>
<tr>
<td>CAT4</td>
<td>Time Sheet: Approve Times (Selection by Org. Assignment)</td>
</tr>
<tr>
<td>CAPP</td>
<td>Time Sheet: Approve Times</td>
</tr>
<tr>
<td>PP61</td>
<td>Change Shift Plan: Entry Screen</td>
</tr>
<tr>
<td>PA61</td>
<td>Maintain Time Data</td>
</tr>
<tr>
<td>PA70</td>
<td>Fast Entry (Time Data)</td>
</tr>
</tbody>
</table>

Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timesheet Entry</td>
<td>Timesheet Approval</td>
<td>A user could enter and approve an inappropriate and/or inaccurate timesheet, resulting in fraudulent payroll payments.</td>
</tr>
<tr>
<td>Timesheet Assessment</td>
<td>Process Payroll</td>
<td>A user could give an incorrect time evaluation and then process the payroll to obtain a fraudulent payment.</td>
</tr>
</tbody>
</table>
Optimising the SAP control environment

Data entry profiles determine the data entry process and the layout of the timesheet. Consideration should be given to the following settings to improve timesheet data entry:

Review Timesheet data entry settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile changeable</td>
<td>Allows a user with access to a profile to change profile settings.</td>
</tr>
<tr>
<td></td>
<td>The recommended setting is: ‘no changes allowed’.</td>
</tr>
<tr>
<td>With:</td>
<td></td>
</tr>
<tr>
<td>Target hours</td>
<td>Available details which may be included on the face of the timesheet.</td>
</tr>
<tr>
<td>Totals line</td>
<td></td>
</tr>
<tr>
<td>Clock items</td>
<td></td>
</tr>
<tr>
<td>Release on saving</td>
<td>On saving time information, consideration should be given to whether it is</td>
</tr>
<tr>
<td></td>
<td>automatically or manually released. It is recommended that this is set to</td>
</tr>
<tr>
<td></td>
<td>manual release.</td>
</tr>
<tr>
<td>Approval required</td>
<td>Workflow configured to ensure time data is subject to appropriate approvals.</td>
</tr>
<tr>
<td>No changes after approval</td>
<td>Should be configured to ensure time data is displayed on the data entry</td>
</tr>
<tr>
<td></td>
<td>screen after approval and cannot be changed.</td>
</tr>
<tr>
<td>Highlight rejected records</td>
<td>Can be configured to show user records that have been rejected by approvers,</td>
</tr>
<tr>
<td></td>
<td>highlighting the need for further action.</td>
</tr>
<tr>
<td>Time settings</td>
<td>Time settings should be configured based on the standard working week.</td>
</tr>
<tr>
<td></td>
<td>This will include defining the number of periods a user can view and change</td>
</tr>
<tr>
<td></td>
<td>(past and future).</td>
</tr>
<tr>
<td>Personnel selection</td>
<td>Defines the profile selection criteria for personnel time data entry.</td>
</tr>
<tr>
<td>Default values</td>
<td>Timesheets can be configured to display default values when accessed.</td>
</tr>
<tr>
<td>Data entry checks</td>
<td>Data entry checks should be configured to improve the quality and</td>
</tr>
<tr>
<td></td>
<td>completeness of data entry. Consideration should be given to applying</td>
</tr>
<tr>
<td></td>
<td>validation tolerances to reduce inaccurate timesheet entry.</td>
</tr>
<tr>
<td>For users with HR</td>
<td>The system should be configured to give an error or warning message when</td>
</tr>
<tr>
<td></td>
<td>interfacing errors occur between CAT and HR.</td>
</tr>
<tr>
<td>Workflow approval</td>
<td>A workflow approval procedure should be configured which will be initiated on</td>
</tr>
<tr>
<td></td>
<td>completion of timesheet entry.</td>
</tr>
</tbody>
</table>
4.3 Payroll Accounting

Payroll calculation and payment overview

The payroll calculation function involves the process of performing the periodic calculation of employee costs, calculation of leave accrual balances, and updating these amounts in the financial records of the entity.

The payroll payment function is the process of approving the payroll calculation for payment to employees and processing the physical payment to the employees, banks, and various vendors (i.e. superannuation payments).
Commonly identified control weaknesses

Control weaknesses that occur in the Payroll accounting process include:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leave accruals</td>
<td>Incorrect leave accruals, particularly where they have been transferred from an external system, are a consistent issue. Rules should be set up to reflect the relevant awards and maximum accrual amounts. Warning messages should be configured where appropriate.</td>
</tr>
</tbody>
</table>

Significant risks

- **High**
  - Incorrect or duplicate payments or ghost employees on the payroll
  - Payroll system does not reconcile to the General Ledger
  - Incorrect changes to pay rates
  - Unauthorised or incorrect manual payments
  - Incorrect leave accruals

- **Medium**
  - Executive payroll is not adequately segregated
  - Incorrect electronic funds transfer (EFT) payments

- **Segregation of duties risk**
  - Payroll Processing and Employee Maintenance
  - Payroll Processing and Payroll Configuration
  - Payroll Processing and Position Management
### Risks and controls

#### R405: Incorrect or duplicate payments or ghost employees on the payroll

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Ghost employees relate to payments to non-existent employees and are the key risk in payroll. Incorrect payment amounts, including the payment of duplicate payments, could lead to the overpaying of employees and/or fraudulent payments, and therefore financial loss to the entity.</td>
</tr>
</tbody>
</table>

#### Controls

**Configuration controls**

*Personnel calculation rules (C1061)*

Personnel calculation rules are used in the calculation of gross and net pay for employees and should be protected from being overridden. These changes should be compliant with the entity’s change control procedures from development to the production environment.

**Manual controls**

*Review Cost Centres Actual / Plan / Variance Report (C296)*

The main risk within any payroll system is the placement of ghost employees on the payroll. Cost centre managers are in the best position to identify ghost employees. Cost centre managers should review report Cost Centres Actual / Plan / Variance (RSSYSTDB), transaction code S_ALR_87013611 to identify any unusual employee payments.

*Review payroll control reports (C585)*

Payroll control reports should be reviewed to identify any unusual or duplicate payments.

#### R406: Payroll system does not reconcile to the General Ledger

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>The payroll system must reconcile to the General Ledger to ensure integrity of the financial statements. If not reconciled, or reconciled incorrectly, there is an increased risk of material misstatement in the financial statements.</td>
</tr>
</tbody>
</table>

#### Controls

**Manual controls**

*Review of Accounting: Payroll Results not Posted Report (C321)*

The posting to Accounting: Payroll Results not Posted report, transaction code PC00_M99_PA03_CHECK, should be regularly reviewed. Payroll results not posted should be actioned.
### R407: Incorrect changes to pay rates

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
</table>

**Risk description**
The integrity of pay rates is critical to ensure correct payroll payments. Incorrect changes may result in over or under-payment.

**Controls**

- **Manual controls**
  - **Recording, authorisation and review of pay rate changes (C314)**
    All changes to pay rate scales should be recorded on a standard form and appropriately authorised. Pay rate changes should be subsequently reviewed to ensure accuracy.

### R408: Unauthorised or incorrect manual payments

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
</table>

**Risk description**
Automated payments are typically more controlled than manual payments. Unauthorised or incorrect manual payments may be processed, leading to overpayment or fraudulent payments.

**Controls**

- **Manual controls**
  - **Review and actioning of the Infotype Audit Report (C621)**
    The Infotype Audit Report (RPUAUD00) is a critical control report within SAP payroll. It is configurable and may be used to review changes to key payroll records. This report should be reviewed and actioned every pay period.
  - **Existence of procedures for one-off or ad-hoc payments (C1062)**
    Procedures should be in place to ensure that one-off or ad-hoc payments are updated in the employee payroll records to ensure that over payments are not processed and all payroll costs are accurately recorded.
### R409: Incorrect leave accruals

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>If long service leave and annual leave accruals are incorrect, then the integrity of the financial statements may be compromised.</td>
</tr>
<tr>
<td>Controls</td>
<td><strong>Configuration controls</strong>&lt;br&gt;1. Consistency and delimiting of leave accrual rules (C1063)&lt;br&gt;Leave accrual rules are used to calculate the leave accruals for each employee. The leave accrual rules should be consistent with employee awards.&lt;br&gt;Each leave accrual rule is delimited by a time period, similar to that used for infotypes. Leave accrual rules that are intended to continue indefinitely should be delimited with the date 31.12.9999.&lt;br&gt;Configuration of maximum values for leave accruals (C1064)&lt;br&gt;Maximum values may be configured for each type of leave accrual. If the maximum leave accrual amount is reached, an error message should be defined and the system will stop accruing further leave.&lt;br&gt;Regular evaluation of leave accrual configuration (C1065)&lt;br&gt;Leave accrual configuration should be regularly evaluated.&lt;br&gt;<strong>Manual controls</strong>&lt;br&gt;Regular review of employees leave accruals should be performed. (C1066)&lt;br&gt;Evaluation of employees with excessive accrual balances. (C1067)</td>
</tr>
</tbody>
</table>

### R410: Executive payroll is not adequately segregated

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Most entities separate executive payroll to avoid inappropriate disclosure of executive salaries. If this is not done, then unauthorised personnel may be able to view executive salaries, resulting in a breach of confidentiality.</td>
</tr>
<tr>
<td>Controls</td>
<td><strong>Manual controls</strong>&lt;br&gt;Use of employee group functionality (C693)&lt;br&gt;It is important to use employee group functionality to restrict security access to key employee groups, such as executives.</td>
</tr>
</tbody>
</table>
R411: Incorrect electronic funds transfer (EFT) payments

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>The majority of payroll payments are processed through electronic funds transfer. Inadequate controls operating over EFT payments may result in incorrect payments and financial loss for the entity.</td>
</tr>
<tr>
<td>Controls</td>
<td>There are a variety of internal controls that must be implemented over the EFT process. Key controls include:</td>
</tr>
<tr>
<td></td>
<td><strong>Configuration controls</strong></td>
</tr>
<tr>
<td></td>
<td><em>Dual authorisation for payments and EFT file security (C340)</em></td>
</tr>
<tr>
<td></td>
<td>• Obtaining dual authorisation for all payments.</td>
</tr>
<tr>
<td></td>
<td>• Ensuring adequate security over the EFT file.</td>
</tr>
<tr>
<td></td>
<td><strong>Manual controls</strong></td>
</tr>
<tr>
<td></td>
<td><em>Reconciliation of transfer of EFT file to system (C340)</em></td>
</tr>
<tr>
<td></td>
<td>• Reconciliation of the transfer of the EFT file from SAP to the payment system.</td>
</tr>
</tbody>
</table>

**Security considerations**

The following table outlines standard Payroll Accounting security objects that should be restricted to appropriate staff:

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td>Description</td>
</tr>
<tr>
<td>PA04</td>
<td>Maintain PA Number Ranges</td>
</tr>
<tr>
<td>PAKG</td>
<td>Adjustments Workbench</td>
</tr>
<tr>
<td>PAUX</td>
<td>Adjustment Workbench</td>
</tr>
<tr>
<td>PC00_M99_CIPE</td>
<td>Create Posting Run</td>
</tr>
<tr>
<td>PC00_M99_PA03_RELEA</td>
<td>Release Payroll</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>P_TCODE</td>
<td>HR: Transaction Code</td>
</tr>
<tr>
<td>P_PCR</td>
<td>HR: Payroll Control Record</td>
</tr>
<tr>
<td>P_PYEVRUN</td>
<td>HR: Posting Run</td>
</tr>
</tbody>
</table>
Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll Processing</td>
<td>Employee Maintenance</td>
<td>An employee could fraudulently change another employee’s bank account or payment details and process a payment to themselves, another employee, or someone outside of the entity.</td>
</tr>
<tr>
<td>Payroll Processing</td>
<td>Payroll Configuration</td>
<td>A user has the ability to change key payroll processing configuration or controls and process a payroll payment.</td>
</tr>
<tr>
<td>Payroll Processing</td>
<td>Position Management</td>
<td>A user with the ability to create a new position and process the payroll could create a ghost employee and process fraudulent payroll payments to that employee.</td>
</tr>
</tbody>
</table>

Optimising the SAP control environment

- Payroll control record
- Payroll exceptions
- Payroll history reconciliation
- Wage types in employee remuneration
- Long service leave
- Transfer employees
- Superannuation
- Payment data transfer
Better practice procedures which should be implemented to ensure that payroll data is entered completely and accurately:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll control record</td>
<td>The payroll control record contains information relating to the payroll period dates as well as the past payroll period up to which retrospective payroll adjustments may be processed. This should be set at an appropriate value to ensure that retrospective adjustments cannot be made too far into the past (i.e. no more than 5 pay periods prior).</td>
</tr>
<tr>
<td>Payroll exceptions</td>
<td>The Payroll Exceptions Report RPCEDT00, transaction code PCO0_M13_CEDT, provides details of any exceptions logged by the system during payroll processing, including any employee master records that contain incomplete information (i.e. missing tax file number). This report should be reviewed to ensure that all data has been entered completely prior to the completion of the payroll run. In addition, this report may assist in identifying any new employees that have been included in the payroll without appropriate authorisation.</td>
</tr>
<tr>
<td>Payroll history reconciliation</td>
<td>Each payroll run should be reconciled to the previous period payroll using the standard reports available. Payroll totals should also be reviewed by Cost Centres to ensure that payroll costs are appropriate and have been completely and accurately processed.</td>
</tr>
<tr>
<td>Wage types in employee remuneration</td>
<td>It is possible to enter additional wage types via the infotype ‘employee remuneration information’. The entry of a wage type through this infotype overrides any existing valuation base for the particular wage type and affects the calculation of employee salary. The system should be configured to specify which wage types may be entered via this screen.</td>
</tr>
<tr>
<td>Transfer employees</td>
<td>Procedures should be implemented to ensure that HR master data history and leave balances are accurately transferred and recorded for employees that transfer from other entities.</td>
</tr>
<tr>
<td>Superannuation</td>
<td>Superannuation calculation rules should be appropriately configured to ensure the correct calculation of Superannuation Guarantee Charge (SGC) amounts.</td>
</tr>
<tr>
<td>Payment data transfer</td>
<td>Appropriate procedures should be implemented to ensure that the file/payments data file created by SAP for sending to the bank/payment authority with the payroll details is not able to be accessed by unauthorised staff. The Bank Deposit Summary report, transaction code S_PH9_46000156, should be produced and sent to the bank/payment authority, along with the data file to enable reconciliation of the SAP payroll data to the actual payments processed by the bank/payment authority.</td>
</tr>
</tbody>
</table>
4.4 Employee Self Service

SAP Employee Self Service (ESS) provides real-time access and data maintenance capabilities to employees. This allows for a reduction in central administration through the assignment of many data entry and related service activities to employees that were previously performed by an entity’s HR, Payroll, Benefits, and Travel departments.

Activities that are performed in ESS include:

- Entry of time sheet information;
- Entry of leave requests;
- Maintenance of personal information;
- Display of pay slips by employees; and
- Display of salary packaging.

ESS enables employees to view, create, and maintain data through a web browser and does not require additional software installations. ESS provides a powerful employee information and service portal through an entity’s intranet.

Commonly identified control weaknesses

The following control weaknesses typically occur in the use of ESS:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inappropriate access allocated through ESS security roles</td>
<td>Distinct security roles are able to be created for access to ESS. These roles often provide additional access to SAP functions, resulting in the ability to process unauthorised SAP transactions and view sensitive data.</td>
</tr>
</tbody>
</table>
Significant risks

- Excessive or unauthorised access to sensitive HR data
- Leave taken is not accurately recorded

Risks and controls

<table>
<thead>
<tr>
<th>R412: Excessive or unauthorised access to sensitive HR data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk rating</strong></td>
</tr>
<tr>
<td><strong>Risk description</strong></td>
</tr>
<tr>
<td><strong>Controls</strong></td>
</tr>
</tbody>
</table>
| | *Configuring ESS security (C1066)*  
ESS security should be designed to restrict users to only having the ability to update non-critical personal data, such as phone number, address, and relevant background information for the user’s profile. Critical HR data, such as bank details, name, and organisational data, should be restricted to the HR department. The display of data should be limited to a user’s entity, department, or position relevant information. |
| | *Defining and assigning of structural authorisation profiles (C1067)*  
Structural authorisation profiles should be defined and assigned to users, ensuring access is appropriately restricted to appropriate organisational units. |
| | *Assigning of all SAP users (C1068)*  
All SAP users must be assigned to an ESS user through infotype 0105 to ensure they are able to only access relevant and appropriate information. |
R413: Leave taken is not accurately recorded

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Employees may take annual or long service leave and the employee’s leave accruals may not be updated. This may result in the employee being granted excess leave, potentially causing financial and resource loss to the entity if undetected. Also, not updating leave accruals may adversely affect the integrity of the financial statements.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
</tbody>
</table>

**Use of standard leave form and appropriate approval of all leave requests (C335)**

A standard leave form should be used to record employees’ requests for leave. All leave requests should be appropriately approved by the employee and the employee’s immediate supervisor.

For entities that rely on employees entering their time in ESS, the leave form should be lodged with the scheduling manager. A review should be performed between leave requests and leave recorded in ESS. Any discrepancies should be followed up.

For entities not relying on ESS for leave time entry, the approved leave form should be sent to payroll for processing.

**Security considerations**

- Structural authorisations are of significant importance when an ESS HR structure is implemented, as they define which activities (create, change or display) a user is permitted to execute. Increased control through *PD Authority Profiles* is critical to the security of employee data. These authorisations define which objects in the organisational plan a user is permitted to access, for example:
  - Entity units
  - Qualifications and requirements
  - Business events

A user’s access to HR data and functionality is made up of traditional SAP authorisations and the HR structural authorisation providing an additional level of security.

- The *PD_ALL* profile should **never be assigned**. This is a full system access profile.

- Each user’s access be restricted to their own employee master record through the “HR: Master data – Check personnel number” (P_PERNR) authorisation object. If the P_PERNR object is not applied, then a user has access to all employee information.

- SAP user master records must be assigned to a SAP HR employee record in order for structural authorisations to operate.
- Access to the following ESS and structural authorisation related sensitive transactions that should be restricted to relevant HR staff:

<table>
<thead>
<tr>
<th>Transaction</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OOSP</td>
<td>Change View “Authorisation Profile”: Overview</td>
<td>Maintain the content of an authorisation profile</td>
</tr>
<tr>
<td>OOSB</td>
<td>Change View “User Authorisations”: Overview</td>
<td>Allocate a user to structural authorisation profile</td>
</tr>
<tr>
<td>HRUSER</td>
<td>Set up and maintain ESS User</td>
<td>Administer ESS users (create, change, delete, password administration, etc.)</td>
</tr>
</tbody>
</table>

**Optimising the SAP control environment**

- Sensitive data

Better practice processes to consider in ESS include:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive data</td>
<td>Each end user should be restricted to viewing only their personal private data and relevant infotypes. Any pertinent HR data, such as bank account, address and name should be maintained only by authorised HR users and should not be updated or changed by the end user.</td>
</tr>
</tbody>
</table>
4.5 Managers Desktop

The Managers Desktop allows managers immediate access to relevant HR, Financial Accounting, and Controlling data. It allows all functional managers to perform administrative tasks for their area of responsibility that may previously have been centralised. The Managers Desktop provides up-to-date information through integrated reports allowing greater management control over personnel.

The Managers Desktop provides a number of ‘Themes’, including:

<table>
<thead>
<tr>
<th>Theme</th>
<th>Theme Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>Employee information reports, including:</td>
</tr>
<tr>
<td></td>
<td>• Entry and approval of travel requirements</td>
</tr>
<tr>
<td></td>
<td>• Education and training data</td>
</tr>
<tr>
<td></td>
<td>• Creation of appraisals</td>
</tr>
<tr>
<td>Entity</td>
<td>Planning and administration reports:</td>
</tr>
<tr>
<td></td>
<td>• Entity maintenance</td>
</tr>
<tr>
<td></td>
<td>• Transfers processing</td>
</tr>
<tr>
<td>Costs and budget</td>
<td>Cost centre accounting functions</td>
</tr>
<tr>
<td></td>
<td>Compensation Management</td>
</tr>
<tr>
<td>Recruitment</td>
<td>Records of decisions related to employee recruitment</td>
</tr>
<tr>
<td>Workflow inbox</td>
<td>Facilitates integration with ESS and approval activities such as:</td>
</tr>
<tr>
<td></td>
<td>• Leave requests and time sheets</td>
</tr>
<tr>
<td></td>
<td>• Expenses</td>
</tr>
</tbody>
</table>

Commonly identified control weaknesses

Control weaknesses that may occur in the Managers Desktop system include:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisational structure</td>
<td>In order for the Managers Desktop to work, it is important that the organisational plan be accurately defined, including the assignment of employees to positions. Incorrect allocation of employees to positions will result in managers gaining inappropriate access to HR data.</td>
</tr>
<tr>
<td>Chief position holders</td>
<td>In order for a user to utilise the Managers Desktop, the user must be the holder of a chief position within the organisational chart. The system uses the chief position indicator to determine the organisational units managed directly and indirectly by the position holder.</td>
</tr>
</tbody>
</table>
Significant risks

- Unauthorised approval of time, expense or other employee or HR data

Risks and controls

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>A user’s time, expenses, or other employee data may be entered and paid without appropriate approval, resulting in incorrect payment or overpayment.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td><em>Organisational structure designed with the proper hierarchy (C1069)</em></td>
</tr>
<tr>
<td></td>
<td>The organisational structure should be designed with the proper hierarchy for each department or organisational unit. A chief position should be defined where appropriate to ensure the appropriate manager is assigned to maintain the group using the Managers Desktop.</td>
</tr>
<tr>
<td></td>
<td><em>Appropriate controls for alternate approvers (C1070)</em></td>
</tr>
<tr>
<td></td>
<td>Appropriate controls should be implemented for the temporary delegation and removal of system access for alternate approvers. These are relevant in the case that a manager is away on leave or otherwise unable to fulfil their typical duties.</td>
</tr>
<tr>
<td></td>
<td>Poor controls regarding delegation of responsibilities may result in excessive access to the system.</td>
</tr>
</tbody>
</table>
Security considerations

Access to the Managers Desktop transaction, PPMDT, should be considered sensitive and restricted to relevant managers. Access to the system operates using dual-level security. A user must have the proper authorisations in their regular user master record as well as the appropriate position profile assigned in SAP HR.

Optimising the SAP control environment

Better practice procedures that should be considered using Managers Desktop system include:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training</td>
<td>Due to the decentralised nature of the system, in-depth training is required to be conducted for all users of the system. This will assist in ensuring that users are aware of the extent of their responsibility and further assist in having transactions approved in a timely manner.</td>
</tr>
<tr>
<td>Managers Desktop ‘Themes’</td>
<td>Managers Desktop ‘Themes’, which grant access to various components of the Managers Desktop functionality, needs to be configured to appropriately restrict information.</td>
</tr>
</tbody>
</table>
Chapter 5

Basis

5.1 Transport Management System 120
5.2 Security 127
5.3 Table and Program Maintenance 146
5.4 Basis System Administration 152
5.5 Mass Maintenance 160
5.6 NetWeaver Security 164
5.7 Central User Administration 167
5.8 Backup and Recovery 169
5.9 Portal Security (SAP Enterprise Portal) 171
IMPORTANT UPDATE
Overview

The Basis component includes client/server architecture and configuration, a relational database management system (RDBMS) and a graphical user interface (GUI). In addition to providing the interface between system elements, Basis includes a development environment for SAP ERP applications and a data dictionary, as well as user and system administration and monitoring.

SAP NetWeaver

When understanding the underlying technology of SAP, it is important to differentiate between the Basis component and new technology, NetWeaver, delivered as part of MySAPNetWeaver. The common differentiator is that Basis manages the ABAP Stack, while NetWeaver manages the Java stack. Traditional SAP components are built using SAP programming language ABAP, while new components are built using Java and sit over a NetWeaver technology platform.

SAP NetWeaver is a set of tools and technologies that provide users with a unified interface between Java and ABAP-based SAP systems. For example, NetWeaver provides the ability to use the SAP Portal to access SAP.

The key Basis and NetWeaver components covered by this guide are:

- **Transport Management System**, which controls change management within an SAP environment.
- **Basis Security**. It is important to secure access to the SAP environment as well as the operating and database system running SAP.
- **SAP Table and Program Maintenance**. SAP internal tables and programs must be effectively managed from a security and performance perspective.
- **System and performance management**.
- **Mass Maintenance**.
- **SAP NetWeaver security**.
- **Central User Management**.
- **System Backup and Recovery**.
5.1 Transport Management System

Change Management is a critical control to ensure that system changes are authorised and appropriately tested before being moved to production.

The Transport Management System (TMS) centralises the configuration for the Change and Transport System (CTS) for all SAP systems. TMS enables a SAP Administrator to manage all SAP change requests from a centralised location (i.e. from one SAP client) and allows pre-defined transport routes to be configured, minimising human error in the import and export of transportable objects.

Commonly identified control weaknesses

Common control weaknesses associated with the Transport Management System include:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inability to apply consistent approval and testing processes for all changes</td>
<td>A consistent change management procedure is often not applied for all changes to SAP systems. Large changes are often effectively managed, however, small changes are not always approved and tested before being transferred into the production system.</td>
</tr>
<tr>
<td>Failure to lock the production system</td>
<td>The SAP production system is not always locked to eliminate the risk of unauthorised modification directly in production.</td>
</tr>
<tr>
<td>Inappropriate approval and management of emergency changes</td>
<td>At times, emergency changes must be made to production systems to address production support issues. Often, retrospective approval and testing of these changes is not performed.</td>
</tr>
<tr>
<td>Failure to apply effective change management within test and quality systems</td>
<td>Often, effective configuration and change management processes are not applied to test and quality systems, which may impact on production system integrity.</td>
</tr>
</tbody>
</table>

Significant risks

- **High**
  - Unauthorised/untested changes are made to the SAP systems
  - Emergency changes are not managed appropriately

- **Medium**
  - Access to test and quality systems is not appropriately restricted
Risks and controls

R500: Unauthorized/untested changes are made to the SAP systems

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>SAP provides the ability to lock the production system and the ability to use the Transport Management System to manage changes made to the production system. To maintain the integrity of the production SAP system, it is important that only authorised changes that have been tested are transferred into production. A key risk is that the production SAP system is not effectively locked from making direct system changes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Controls</th>
<th>Configuration controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Production and test clients</strong></td>
<td>All production and test clients should be set to prevent changes to the customising settings for the client. All customising settings specific to the client should be locked. However, this does not lock ‘current settings’ such as exchange rates and posting periods, which need to be regularly maintained. (C677)</td>
</tr>
<tr>
<td><strong>CTS configuration</strong></td>
<td>Changes that are made to CTS configuration tables in all environments should be documented and should only be performed on the basis of authorised requests. Changes to these tables should follow the normal change control procedures. This should include regular review of the table change report. Custom development classes should be configured to ensure that all objects associated with the relevant development class are subject to change control procedures and the use of the CTS. (C1071)</td>
</tr>
<tr>
<td><strong>Production environment settings</strong></td>
<td>Company code(s) for the production environment should be set to ‘productive’ to help prevent unauthorised change. (C704) This restricts the ability to process a client copy (remote copy) into the production system. (C787) It is important to restrict the ability to change cross client objects. This should be restricted in the production client. (C784)</td>
</tr>
</tbody>
</table>
R500: Unauthorised/untested changes are made to the SAP systems (continued)

Manual controls

⚠️ Documenting of change control procedures (C669)

Change control procedures should be documented to ensure that all changes are performed according to consistent standards. Procedures must address all aspects of change control for the SAP system, including:

- master data that cannot be transported via the CTS;
- emergency change procedures;
- ABAP programs and custom code;
- configuration elements (system settings);
- configuration elements that can only be updated online in the production environment;
- SAP supplied code, including patches and OSS notes (corrections for SAP bugs/errors);
- identification of criteria for any overrides to the CTS and alternative procedures to follow;
- version control;
- other change management documentation;
- review and approval procedures;
- use of audit trail reports; and
- testing requirements.

In addition, the procedures document should:

- define individual responsibilities and tasks that are required during the change process;
- determine how the SAP transport and correction process is managed;
- assess the adequacy of policies, procedures and standards, including the execution of SAPSTART and STOPSAP programs;
- identify the development standards that are in place, including naming conventions and development class assignment for security, programs, transactions and screens; and
- transport paths should be set up so that only valid systems can be transported into production.
R500: Unauthorised/untested changes are made to the SAP systems (continued)

*Reports to assist in monitoring the change control process (C1072)*

There are standard reports available in SAP that can assist in monitoring the change control process, including:

- *Overview of repairs* – this report is executed via the development workbench and displays a list of corrections and customising requests according to the selection criteria entered. This may be useful in monitoring repairs and change requests in the system;

- *List of objects modified by user DDIC* – this report provides a list of objects that have been modified by this special SAP user and should be reviewed regularly to ensure that no unauthorised changes have been made using this powerful standard user; and

Changes to sensitive system customising tables (including CTS tables) should be logged in both the development and production environments and the report *Analysis of table log database* should be regularly reviewed to ensure that any unauthorised table changes are detected.

R501: Emergency changes are not managed appropriately

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Emergency changes are made to production systems to address production support issues. Weaknesses in change management procedures may mean that retrospective approval and testing of these changes is not performed.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td>1. <em>Restriction of emergency fixes in the production system</em></td>
</tr>
<tr>
<td></td>
<td>Emergency fixes in the production system should be restricted and performed only if absolutely necessary. The change management procedures and processes should ensure that emergency changes are approved and tested. (C1073)</td>
</tr>
</tbody>
</table>
## R502: Access to test and quality systems is not appropriately restricted

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Given modifications to production systems and configurations are transported from test and quality systems, inappropriate security controls operating within the test or quality system can result in the transport of an unauthorised program into the production system.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td>Preventing changes to client-independent tables</td>
</tr>
<tr>
<td></td>
<td>All production and test clients should be set to prevent changes to client independent tables to ensure the integrity of system data. (C786)</td>
</tr>
<tr>
<td></td>
<td>Preventing changes to ABAP programs and development objects</td>
</tr>
<tr>
<td></td>
<td>All production and test clients should also be set to prevent any changes to ABAP programs and development objects. This will ensure the integrity of system data and programs. (C786)</td>
</tr>
<tr>
<td></td>
<td>Consistency of settings in CTS configuration tables</td>
</tr>
<tr>
<td></td>
<td>Settings in the CTS configuration tables should be consistent across all environments to ensure the correct operation of the CTS and the entity’s change control procedures. (C1074)</td>
</tr>
</tbody>
</table>
Security considerations

The integrity of the Transport Management System and change management process relies on restricting access to key change management functions.

Key security considerations include:

- **Access to the Workbench Organiser should be restricted.** All changes should be controlled by the use of the CTS and this should be restricted from developers in all environments.

- **Developers/programmers should be restricted from releasing development requests for export.** This role should be performed by the system administrator or user responsible for performing the transports.

- **Access to modify the CTS tables could allow users to by-pass controls designed into the Workbench Organiser. These tables should be restricted in all environments.**

Access to the following transport management transactions and authorisation objects should be restricted:

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transactions</strong></td>
<td></td>
</tr>
<tr>
<td>SE01</td>
<td>Transport Organiser (Extended)</td>
</tr>
<tr>
<td>SE09</td>
<td>Workbench Organiser</td>
</tr>
<tr>
<td>SE10</td>
<td>Transport Organiser</td>
</tr>
<tr>
<td>STMS</td>
<td>Central User Management</td>
</tr>
<tr>
<td><strong>Authorisation Objects</strong></td>
<td></td>
</tr>
<tr>
<td>S_TRANSPORT</td>
<td>Transport changes</td>
</tr>
<tr>
<td>S_CLNT_IMP</td>
<td>Data import for client copy</td>
</tr>
<tr>
<td>S_TABU_CLI</td>
<td>Maintain client independent tables</td>
</tr>
<tr>
<td>S_PROGRAM</td>
<td>ABAP/4 program checks</td>
</tr>
<tr>
<td>S_DEVELOP</td>
<td>ABAP/4 development tools</td>
</tr>
<tr>
<td>S_QUERY</td>
<td>Ad hoc queries</td>
</tr>
<tr>
<td>S_RZL_ADM</td>
<td>SAP ERP administration authorisation</td>
</tr>
</tbody>
</table>
Optimising the SAP control environment

Optimising SAP controls

- Implementation of an automated change management system

Better practice elements to consider for Transport Management include:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation of an automated change management system</td>
<td>An automated change management system should be implemented to record approvals for changes and to manage the transport process.</td>
</tr>
</tbody>
</table>
5.2 Security

Effective IT security controls ensure that financial reporting systems and subsystems are appropriately secured to prevent unauthorised use, disclosure, modification, damage or loss of data. Managing systems security includes both physical and logical controls that prevent unauthorised access. These controls typically support authorisation, authentication, non-repudiation, data classification and security monitoring.

Functional overview

Many aspects of SAP security need to be considered, including security administration, maintaining global security parameters, securing access to data and programs, restricting access to standard profiles and authorisations, limiting the use of super users, protecting access to system tables and segregating functions within the system.

This section of the guide addresses key SAP security administration elements, including the ability to maintain security roles and user security, as well as special security parameters and capabilities.

Security related to individual SAP components has been covered separately as a component of each section of this guide.

Security elements and associated risk

There are many elements of a SAP technical environment that creates security risk.

- **Operating system security.** The security risks associated with the operating system are typically limited to a small number of system administrator type users.

- **Database security.** The security risks within the database level are typically limited to a small number of database administration users.

- **Single sign-on and NetWeaver access and security.**

- **Internal SAP security.** This is the key area of security risk. A large number of users have access to the SAP system and can use inappropriate access rights to process inappropriate and unauthorised payments.

The majority of SAP security risks are focused within the SAP system.
Commonly identified control weaknesses

The following control weaknesses typically occur with the implementation and management of SAP security:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segregation of duties concerns</td>
<td>It is important to segregate the ability to perform functions that can be used in conjunction to process fraudulent transactions, such as the ability to create a ghost vendor and process a payment. Often, key segregation of duties risks are not understood and access to conflicting functions is not restricted.</td>
</tr>
<tr>
<td>Inadequate restriction of user access to critical functions</td>
<td>Access to critical functions such as master data maintenance, including the maintenance of vendor accounts or user security maintenance, is often not adequately restricted.</td>
</tr>
<tr>
<td>Entity structure security</td>
<td>Access to sensitive elements of an entity is typically restricted using entity element security within SAP. Often, security is inadequately configured to restrict access to sensitive areas.</td>
</tr>
</tbody>
</table>
| Cross-Talk | Cross-Talk relates to the underlying principle of SAP security where an authorisation with the greater level of access will override lower level access granted in another authorisation. Cross-Talk is a major concern, particularly when access needs to be segregated by company code. For example, a user has been allocated the following two authorisation values for object F_BKPF_BUK:  
  - Authorisation 1: Provides access to only company 0001; and  
  - Authorisation 2: Provides access to all companies.  
  The user will have access to all companies, because authorisation 2 overrides specific security granted in authorisation 1. |
| Reference users | SAP security provides the ability to create reference user accounts which can be allocated to provide new access to existing or new users. The users adopt the access privileges of the reference user. This is a significant risk if reference user allocations are not effectively managed. |
| Security administration process | The security administration process, including the process for maintaining security roles and user access, often does not include preventative checking for segregation of duties conflicts when making changes. |
Cross-Talk in SAP Security

Cross-Talk is a limitation of the SAP security structure whereby a user is granted additional, unintended access such as the ability to create, delete, change, or view documents, postings and other significant information in unintended areas.

A user’s master record is a compilation of profiles, transaction codes (T-Codes), and authorisations (Auth Objects). Since SAP security is additive and SAP Profiles are not self-contained, any authorisation contained in one profile is active across all profiles assigned to the user. When SAP checks a user’s master record, it looks at the overall pool of T-Codes, Auth Objects and object values contained across the user’s profiles. Therefore, the combination of authorisations could unintentionally allow a user access to incorrect data.

The example below highlights how an AP clerk, who is also assigned a display role, is inadvertently given the ability to post new General Ledger documents:

<table>
<thead>
<tr>
<th>Role/ Profile:</th>
<th>Z_AP_CLERK</th>
<th>Z_FI_DISPLAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Object</td>
<td>S_TCODE</td>
<td>F_BKPF_BUK</td>
</tr>
<tr>
<td>Field</td>
<td>TCD</td>
<td>ACTVT</td>
</tr>
<tr>
<td>Values</td>
<td>F-43, 01</td>
<td>1000</td>
</tr>
</tbody>
</table>

The intent of Z_FI_DISPLAY is to give display only access to FB50 (GL Account Posting). However, due to the collision of the two profiles, this AP clerk can now not only view (03) but can also post (01) new GL documents through FB50!

The user’s Master Record in SAP’s view actually looks like this:

<table>
<thead>
<tr>
<th>Auth Object</th>
<th>S_TCODE</th>
<th>F_BKPF_BUK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>TCD</td>
<td>ACTVT</td>
</tr>
<tr>
<td>Values</td>
<td>F-43, FB50</td>
<td>01, 03, 1000</td>
</tr>
</tbody>
</table>

Notice the values for F_BKPF_BUK. It now shows both activity 03 and 01 for company code 1000. This is true for ANY instance where this Auth Object is called.

The most obvious place for Cross-Talk to occur is when the star (*) value is used. This is especially dangerous if (*) is given for S_TCODE, allowing a user to access all or a large range of T-Codes. Cross-Talk is not limited to objects containing a company code field (BUKRS). It also applies to other common fields such as account type (KOART), business area (GSBER) and all other entity values.

Source: Protiviti Australia
**Monitoring for Cross-Talk issues which result in problems with access across organisational areas**

An entity (Entity A) entered into an agreement with a separate independent entity (Entity B) to allow them to use their SAP instance as their financial system.

Entity A provides SAP services on a fee for service basis. One of the key contractual clauses established within the agreement was that access to Entity B’s systems must be restricted.

Entity B was established using a company code structure and access to their company code was restricted. Only two staff members from Entity A were allowed access to the Entity B company code for support purposes.

The way SAP security works causes problems with implementing effective entity level security. Given SAP security simply takes all access provided by all security roles allocated to a user together, this results in specific allocated access being overridden in certain instances. For example, if in one security role a user is allocated access only to Entity A, but then in any role the user is accidentally given access to all companies, then the user will have access to Entity B.

In this instance, when implementing the shared service arrangement, Entity A created a separate set of security roles which only provided access to the Entity B system.

One area that caused problems was in the invoice entry area. Only users working in Entity B were given access to invoice entry in the Entity B company code. There was one display role, however, which accidentally provided create access to all companies. This role was allocated to all Entity A users and provided them with access to process invoices in Entity B.

The user used this access to process an unauthorised invoice in the Entity B system, resulting in Entity A breaching their contract with Entity B.

Source: Protiviti Australia
Significant risks

- Incorrect implementation of administration/ownership policy
- Inappropriate security administration processes
- Ineffective established security parameters
- Inappropriate access to key SAP privileges
- Access is allocated to incompatible transactions

Risks and controls

**R503: Incorrect implementation of administration/ownership policy**

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Failure to allocate effective ownership of key risk areas can result in insufficient segregation of duties and inappropriate access to critical data.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
</tbody>
</table>

**SAP program and data ownership**

SAP program and data ownership should be formally identified and assigned to a specific role in the entity. (C1075)

**Access requests approvals**

Access requests should be approved by the relevant data/profile owners (rather than just the line manager). This may mean the request requires approval from multiple data owners. (C1076)

**Documentation of SAP program and data ownership**

SAP program and data ownership should be documented and the documentation should specifically deal with the various elements of data (i.e. system files, tables). Documentation should include instructions on how data owners should approve access to data within their area of responsibility. (C1077)

**Data administration function**

A data administration function should also be defined with the responsibility for maintaining SAP data, system tables and the data dictionary, and liaising with end users. (C1078)
### R503: Incorrect implementation of administration/ownership policy (continued)

<table>
<thead>
<tr>
<th>Identification of critical elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical elements, including sensitive organisational areas and critical transactions, should be identified. (C1079)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consideration of segregation of duties issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segregation of duties issues should be considered in the establishment of data administration duties. Data administration staff should not be authorised to enter transaction data or update master files. (C1080)</td>
</tr>
</tbody>
</table>

### R504: Inappropriate security administration processes

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Failure to implement effective security administration processes can result in the allocation of unauthorised or inappropriate SAP access.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Controls</th>
<th>Manual controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documenting SAP security procedures and including task related procedures</td>
<td>SAP security administration procedures should be documented and include procedures to address the following tasks:</td>
</tr>
</tbody>
</table>

- Addition, changing and deletion of user access privileges.
- Requirement to perform preventative checking for segregation of duties when allocating access.
- Access to the SAP system, which should be authorised and approved in writing by the relevant data or process owners.
- Removal of access for temporary staff (i.e. contractors). This can be achieved via the use of validity periods on the user master records.
- Deletion of users who have never logged in, have not logged in for a certain number of days or who have left the entity. Consideration should be given to locking out users who have not logged on in over 30 days.
- Automatic notification of security administration staff when an employee leaves the entity or is transferred to a new position to enable them to remove SAP access, as well as access to other systems (i.e. operating system, local area network).
- Removal of access to the SAP system when access to other systems (operating system, local area network) is removed.
- Use of reports of security administration activity.
- An audit trail of security administration activity should be reviewed on a regular basis in order to detect any unusual activity.
- A periodic review should be performed of the access rights assigned to each user to ensure that adequate segregation of duties is maintained and access to critical functions is appropriate.
- Maintenance of user group records.
- Documentation, approval and maintenance of mitigating controls. (C682, C640, C639) |
**R505: Ineffective established security parameters**

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>SAP provides system parameters that define the way the SAP system operates, particularly system logon and password maintenance functions. Incorrect configuration of system parameters can result in security exposures.</td>
</tr>
<tr>
<td>Controls</td>
<td><strong>Configuration controls</strong></td>
</tr>
</tbody>
</table>

**Key system parameters from a security and control perspective**

The following table outlines key system parameters that are critical from a security and control perspective. (C647)

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description / Importance of Setting</th>
<th>Default Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/fails_to_session_end</td>
<td>Number of times a user can enter an incorrect password before SAP stops the session.</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>login/fails_to_user_lock</td>
<td>Number of times a user can enter an incorrect password before SAP locks the user master records from further logons. Locked users are automatically unlocked by SAP at the end of the day. This means that each day a user can try to log on 11 times before being locked.</td>
<td>12</td>
<td>5</td>
</tr>
<tr>
<td>login/min_password_length</td>
<td>Sets the minimum password length.</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>login/password_expiration_time</td>
<td>Users are forced to change their SAP password after a certain number of days.</td>
<td>0</td>
<td>90</td>
</tr>
<tr>
<td>rdisp/gui_auto_logout</td>
<td>Permitted period of inactivity before SAP automatically logs off terminals not actively using SAP.</td>
<td>0</td>
<td>600</td>
</tr>
<tr>
<td>auth/no_check_in_some_cases</td>
<td>If set to Y, it allows the users through transaction SU24 to switch off authorisation checks for selected transactions. This is a required setting to be able to use the profile generator.</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>login/disable_multi_gui_login</td>
<td>This parameter can deactivate multiple user logins. If set to 1 multiple logins are blocked.</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
### R505: Ineffective established security parameters (continued)

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description / Importance of Setting</th>
<th>Default Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/min_password_diff</td>
<td>This parameter defines how many characters in the new password must differ from the old password.</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>(New with ECC6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/min_password_digits</td>
<td>This parameter specifies the minimum number of digits that a user's password must contain.</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(New with ECC6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/min_password_letters</td>
<td>This parameter specifies the minimum number of letters that a user's password must contain.</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(New with ECC6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/min_password_specials</td>
<td>This parameter specifies the minimum number of special characters that a user's password must contain.</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>(New with ECC6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/password_max_new_valid</td>
<td>Defines the number of days before an initial password set up for a new user expires.</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>(New with ECC6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>login/password_max_reset_valid</td>
<td>Defines the number of days before a reset user's password expires.</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>(New with ECC6)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Single sign-on for SAP systems

The SAP ERP Central Component and the SAP NetWeaver both support several variations of single sign-on mechanisms. SAP ERP supports the single sign-on (SSO) mechanisms provided by the NetWeaver ABAP Application Server. Therefore, the parameters for user management and authentication used by the SAP NetWeaver Application Server also apply to the SAP ERP Central Component.

The most popular user authentication mechanisms supported by SAP include:

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID and Password</td>
<td>Default mechanism to use for user authentication for both SAP and Internet protocols, regardless of the frontend client.</td>
</tr>
<tr>
<td>Secure Network Communications (SNC)</td>
<td>Used for user authentication and single sign-on when using SAP protocols (dialog, RFC) and the SAP GUI for Windows or SAP GUI for Java as the frontend clients. Transport layer security is also provided when using SNC.</td>
</tr>
<tr>
<td>Logon Tickets</td>
<td>Used for single sign-on when using internet protocols and a web browser as the frontend client.</td>
</tr>
<tr>
<td>SSL and X.509 Client Certificates</td>
<td>Used for both user authentication and single sign-on when using internet protocols and a web browser as the frontend client.</td>
</tr>
</tbody>
</table>

For more information and configuration assistance, visit the SAP Library at http://help.sap.com/. The User Authentication and Single Sign-On section of the SAP NetWeaver Security Guide provides detail and example configurations.

Single sign-on increases the likelihood of an anonymous user gaining access to the system through an authorised user’s machine. Entities should undertake measures to prevent this from happening, including using HTTPS communication paths and defined DNS domains, as well as instituting a policy that requires the use of password-protected screen savers and procedures for manually locking the workstation when users leave their desk.

Source: Protiviti Australia
### R506: Inappropriate access to key SAP privileges

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>High level privileges, such as SAP_ALL, provide full access to the SAP system. Inappropriate use of these privileges can result in the processing of unauthorised or fraudulent transactions.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
</tbody>
</table>

#### Restricting access to key privileges

Access must be restricted to the following key privileges:

- The SAP* user is delivered as the standard super user with the system. It should not be deleted because it will be reinstated by the system with a default password which is widely known and easily guessed. SAP recommends that the SAP* user be copied to another user master record (this will become the super user to provide emergency access privileges), and the profiles allocated to SAP* removed to reduce further the likelihood of unauthorised access. (C655)
- DDIC user ID is provided by SAP and is used in a number of background SAP jobs. This user account provides extensive access and access must be restricted. (C662)
- Access to the SAP_ALL profile should also be restricted. This profile allows the user to perform all functions in the system and is especially powerful. It should not be granted to any users in the production environment. (C662)
- All authorisations for newly created objects (SAP_NEW). This profile provides general access to any new profiles and authorisations which are included in a new release of SAP. (C661)
### R507: Access is allocated to incompatible transactions

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Restricting access to incompatible transactions reduces the risk that fraudulent transactions can be processed. If a user has access to incompatible transactions, they could initiate an unauthorised or fraudulent transaction.</td>
</tr>
<tr>
<td>Controls</td>
<td>The following controls and procedures should be implemented to eliminate access to incompatible functions in the production system:</td>
</tr>
<tr>
<td>Configuration controls</td>
<td><strong>Eliminating access to combinations of transactions</strong></td>
</tr>
<tr>
<td></td>
<td>It is imperative to eliminate access to combinations of transactions that can facilitate fraudulent processing of transactions to reduce the risk of fraud. For example, the ability to change a vendor’s bank account and then process a payment to that bank account must be restricted. (C1081)</td>
</tr>
<tr>
<td></td>
<td><strong>Assessing security roles design</strong></td>
</tr>
<tr>
<td></td>
<td>As part of the security implementation project, security roles design should be assessed to determine whether they provide access to conflicting duties in the system. Care should be taken to ensure that security roles created provide only the level of access which is intended by management. (C1082)</td>
</tr>
<tr>
<td>Manual controls</td>
<td><strong>Performing preventative segregation of duties checks</strong></td>
</tr>
<tr>
<td></td>
<td>Security management procedures should include the process of performing preventative segregation of duties checks during the creation and modification of security roles and user access. (C1083)</td>
</tr>
</tbody>
</table>

### R508: Unauthorised OSS access

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>OSS access is used by SAP to provide emergency support. Unauthorised OSS access for support activities can result in inappropriate changes to the SAP system.</td>
</tr>
<tr>
<td>Controls</td>
<td><strong>Configuration controls</strong></td>
</tr>
<tr>
<td>OSS settings</td>
<td>OSS accounts are usually established within the SAP system to allow SAP to support the product in case of application issues. OSS accounts usually have significant access; access to these accounts must be adequately restricted. Key controls typically implemented include locking the account when not in use and dial back capabilities to ensure the authenticity of the remote access user. (C859)</td>
</tr>
</tbody>
</table>
### R509: Inappropriate access to SAP utilities

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>SAP standard utilities, such as spool and batch files utilities, are potentially powerful and can be used for unauthorised purposes.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>Restricted access to SAP standard utilities</strong></td>
</tr>
<tr>
<td></td>
<td>Access to such tools should only be restricted to key administration personnel and/or granted on an as required basis. (C663)</td>
</tr>
</tbody>
</table>

### R510: Inappropriate derived role maintenance and configuration

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Derived roles are inappropriately configured, resulting in inappropriate user access. Due to limitations of organisational data that can be derived, there are certain situations where derived roles cannot be used. Where derived roles are used and all data (with the exception of organisational data) is to be derived down to the child role, child roles should not be directly maintained. All changes to the child role will be overwritten the next time information is derived from the master role.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>Non-assigning of master role to end users</strong></td>
</tr>
<tr>
<td></td>
<td>Where derived roles have been defined, the master role should not be assigned to end users as this will normally contain access to all organisational data. (C1084)</td>
</tr>
<tr>
<td></td>
<td><strong>Restricted access to the profile generator</strong></td>
</tr>
<tr>
<td></td>
<td>Only security administration staff should have access to the profile generator (transaction PFCG) where derived roles are maintained. (C1085)</td>
</tr>
<tr>
<td></td>
<td>** Appropriately defined and clear naming conventions**</td>
</tr>
<tr>
<td></td>
<td>Ensure that naming conventions have been appropriately defined which clearly identify master and child roles. (C1086)</td>
</tr>
</tbody>
</table>
R511: Insufficient reporting security

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
</table>

Risk description

With the increased use of personalised roles, reporting security has changed significantly. In previous versions of SAP, reports were secured by attaching them to a report tree. Report trees were then allocated to users to ensure users could only access approved reports.

Since folders can be specified in individual roles, personalised roles effectively make reporting trees redundant. In order to make the allocation of reports to roles easier, SAP have therefore assigned a large number of standard SAP reports to transaction codes.

Although report trees can still be displayed through most web GUI configurations, it may be more appropriate to assign reports through personalised roles, and remove report trees altogether.

Controls

**Configuration controls**

*Establishment and allocation of required authorisation objects*

The key configuration risk relating to reports is to ensure that, although transaction codes have now been assigned to SAP standard reports, the authorisation objects checked by these reports have not been attached to these transaction codes. In order to allocate reports to end users, it is therefore still necessary to establish the required authorisation objects through testing and allocate these to the appropriate roles.

Reports which do not contain adequate authorisation object security will be accessible to any user who has access to the transaction code required to start the report. Where users are configured with access to all transaction codes, through the application of a ‘*’ in the S_TCODE object, or value that contains a ‘*’ (for example ‘S*’), there is an increased risk that reports or programs may be accessed inappropriately. (C1087)
### R512: Use of standard SAP roles or profiles

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>SAP comes with a number of standard security roles and profiles that can be used by the entity. These standard profiles and authorisations should not be used in production. This is because the access they provide is extremely generic and, generally, do not adequately address segregation of duties issues.</td>
</tr>
</tbody>
</table>

**Controls**

**Configuration controls**

*Limiting allocation of standard roles or profiles*

Standard roles or profiles should not be allocated to users. Standard roles or profiles can be used as a basis for creating custom roles, however, they must be separately assessed for segregation of duties concerns before use. (C1088)

### R513: Inappropriate operating system access

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Inappropriate access to operating system privileges can result in damage being caused to the SAP system.</td>
</tr>
</tbody>
</table>

**Controls**

**Configuration controls**

*Restricted access to operating system privileges*

SAP can run on a variety of operating systems, primarily being run on UNIX. SAP users do not need direct logons to the operating system to gain access to SAP. Access must be restricted to operating system privileges to ensure the integrity of the SAP system. (C1089)

### R514: Unauthorised database access is obtained

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Inappropriate access to database privileges can result in damage being caused to the SAP system.</td>
</tr>
</tbody>
</table>

**Controls**

**Configuration controls**

*Restricted access to key database privileges and capabilities*

A variety of different databases are used by clients with the SAP system. These include SQL Server and Oracle. Access to key database privileges and capabilities must be appropriately restricted. (C1090)
Security considerations

Key security considerations include:

- Authorisations where a ‘*’ value has been given should be reviewed to establish if appropriate. Where possible, such values should be limited and replaced with specific values to prevent the assignment of excessive access.

- Access to perform security administration functions, including the profile generator, should be restricted. This is controlled via the following authorisation objects:
  - S_USER_GRP – User master maintenance: User groups;
  - S_USER_PRO – User master maintenance: Authorisation profile;
  - S_USER_AUT – User master maintenance: Authorisations; and
  - S_TCODE – Authorisation check for transaction start.

- In addition, the security parameter ASSIGN_ROLE_AUTH is new in ECC5 / ECC6. The parameter is used to segregate in Profile Generator the ability to assign a role to a user from the ability to modify a role. This segregation is provided only if the parameter is set to ‘Assign’.

If ASSIGN_ROLE_AUTH is set to CHANGE then the following authorisations are required to assign a role to a user:

- S_USER_GRP, activity 22 (assign)
- S_USER_AGR, activity 02 (change)

If ASSIGN_ROLE_AUTH is set to ASSIGN then the following authorisations are required to assign a role to a user:

- S_USER_GRP, activity 22 (assign)
- S_USER_AGR, activity 22 (assign)

- SAP security may be administered in a centralised or decentralised manner (i.e. at one location or many). In either case, it is important that there is adequate segregation of duties between the security administrators. There are three security administration roles defined in SAP:
  - User administrator (defines and maintains user master records);
  - Authorisation administrator (maintains profiles/activity groups and authorisations); and
  - Activation administrator (activates/generates profiles and authorisations).

Authorisation and activation administration should be performed in the development environment. Segregation of the activation and authorisation administration roles provides a strong control over the accuracy and authorisation of changes. Where not segregated, a measure of control can be achieved via independent review of reports of changes to profiles and authorisations.

- Security administrators may grant themselves access to inappropriate transactions. They can be restricted from maintaining their own access rights, however, they would still be able to create a new user master record. This could be used to access inappropriate transactions. Security administrator access can only be fully restricted if SAP is linked to an external security system (i.e. SECUDE or KERBEROS).

- As with access to all user administration functionality, access to role maintenance activities should be controlled.
Access should be restricted to the following transactions which provide users with access to role and profile maintenance activities:

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Items</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Transactions</strong></td>
<td>Description</td>
</tr>
<tr>
<td>PFCG</td>
<td>Profile Generator</td>
</tr>
<tr>
<td>SU01</td>
<td>Maintain User</td>
</tr>
<tr>
<td>SU02</td>
<td>Profile Maintenance</td>
</tr>
<tr>
<td>SU03</td>
<td>Authorisation Maintenance</td>
</tr>
<tr>
<td>SU10</td>
<td>User Mass Maintenance</td>
</tr>
<tr>
<td>SU20</td>
<td>Maintain Authorisation Fields</td>
</tr>
<tr>
<td>SU21</td>
<td>Maintain Authorisation Objects</td>
</tr>
<tr>
<td>SU22</td>
<td>Authorisation Object usage in transactions</td>
</tr>
<tr>
<td>SU12</td>
<td>Mass Changes to User Master Records</td>
</tr>
<tr>
<td>P013</td>
<td>Role Assignment to Positions</td>
</tr>
<tr>
<td>OY21, GCE2, O002, OBZ8, OD03, OIBP, OMDM, OMEI, OMMO, OMSO, OMWG, OOPR, OP15, OPCB, PFCG</td>
<td>Role Maintenance for Derived Roles</td>
</tr>
<tr>
<td><strong>Authorisation Objects</strong></td>
<td></td>
</tr>
<tr>
<td>S_USER_GRP</td>
<td>User Maintenance by Group</td>
</tr>
<tr>
<td>S_USER.PRO</td>
<td>Role(Profile Maintenance)</td>
</tr>
<tr>
<td>S_USER.AUTH</td>
<td>Authorisation Maintenance</td>
</tr>
<tr>
<td>S_USER.AGR</td>
<td>User Activity Groups</td>
</tr>
<tr>
<td>P_ORIGIN</td>
<td>Checks for HR data</td>
</tr>
<tr>
<td><strong>Standard Reports</strong></td>
<td></td>
</tr>
<tr>
<td>S_BCE_68001425</td>
<td>Roles by Complex Criteria</td>
</tr>
<tr>
<td>S_BCE_68001418</td>
<td>Roles by Role Name</td>
</tr>
<tr>
<td>S_BCE_68001420</td>
<td>Roles by Transaction Assignment</td>
</tr>
<tr>
<td>S_BCE_68001419</td>
<td>Roles by User Assignment</td>
</tr>
<tr>
<td>S_BCE_68001421</td>
<td>Roles by Profile Assignment</td>
</tr>
<tr>
<td>S_BCE_68001422</td>
<td>Roles by Authorisation Object</td>
</tr>
<tr>
<td>S_BCE_68001423</td>
<td>Roles by Authorisation Values</td>
</tr>
<tr>
<td>S_BCE_68001424</td>
<td>Roles by Change Data</td>
</tr>
</tbody>
</table>
Optimising the SAP control environment

Better practice items to consider in the set up and management of security include:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derived roles</td>
<td>Derived roles – The profile generator controls the creation of variants for different business units or departments within an entity. This has resulted in the concepts of responsibilities (Version 4.0B), hierarchical activity groups (Version 4.5A) and, more recently, derived roles (Version 4.6A). All are conceptually similar in that they allow the security administrator to define a set of common transactions from which variant profiles can be created containing different organisational restrictions. It should be noted that the use of derived roles can significantly reduce the resource required for security role maintenance. These can be further explained using the following diagram:</td>
</tr>
</tbody>
</table>

![Diagram showing derived roles](Diagram.png)
<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard SAP menu</strong></td>
<td>Turning the SAP standard menu off reduces the risk that a user will accidentally select a menu item that they should not be accessing. The ideal configuration is set to <strong>Yes</strong>, which means that the SAP menu would be turned off.</td>
</tr>
<tr>
<td><strong>Password generation capabilities of SU01</strong></td>
<td>Password generator functionality is included in transaction SU01. This allows the security administrator to generate a random password for user accounts, rather than a password which may be easily guessed.</td>
</tr>
</tbody>
</table>
| **PRG_CUST settings**                         | This is a new system security parameter that has been introduced in ECC5/6. The parameter allows access to assign roles and maintain roles to be segregated.  

The ASSIGN_ROLE_AUTH should be set to value ASSIGN so that the authorisation values required for assigning roles to users do not also grant the ability to modify the authorisations of the role. |
| **Security audit log**                        | SAP provides a security monitoring log that can be used to identify unusual user activity. The security audit log is configured with filters which can be defined to include specific users, SAP system clients, audit class (activity to be logged), and weight of event (i.e. critical or important).  

Key events to consider logging include: user login failed; changes to user master records or security authorisation data; and all activity of super user accounts such as SAP* and DDIC.  

Security audit logging can have a significant impact on SAP system performance. Therefore, it is extremely important to determine the most optimal security logging strategy that both achieves audit objectives and minimises the impact on system performance. |
| **Document type authorisation groups**         | Document type authorisation groups should be set for sensitive document types. These authorisation groups can then be allocated to key users responsible for these document types. |
| **Use of user groups**                        | Users can be assigned to pre-defined user groups in their user master record. These groups do not have a system impact on SAP security authorisations; however, they are an extremely useful tool for identifying users by business unit, location or department for both operational and audit purposes. |
| **Define illegal passwords**                  | SAP has the functionality to define passwords that are easy to guess and should not be used in SAP table USR40. This restricts the ability of users to use easily guessable passwords such as the company name or days of the week. |
User versus position based security

User based security, or direct role assignment, is the assignment of access rights to an individual user, who performs certain actions on behalf of their entity. SAP security roles are assigned directly to the User ID. A user can be assigned one or multiple security roles.

Position based security, or indirect role assignment, is the assignment of access rights to a HR position, rather than to an individual user. When a user is allocated to a position by HR, they automatically inherit the access that has been assigned to that position.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>User Based Responsibility</th>
<th>Position Based Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>User changes position and security access is not removed</td>
<td>Entities typically rely on role owners or a manager to inform the security group when a user changes position. The users typically gain the access required for the new position without relinquishing their existing access.</td>
<td>With position based security, as soon as a user is moved positions in the entity structure, that user loses their existing access and gains the access required for the new position.</td>
</tr>
</tbody>
</table>

Key advantages and limitations of the security methodologies:

<table>
<thead>
<tr>
<th>Advantages</th>
<th>User Based Security</th>
<th>Position Based Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reduced complexity</td>
<td>Improved security administration</td>
</tr>
<tr>
<td></td>
<td>Increased flexibility</td>
<td>Improved compliance</td>
</tr>
<tr>
<td></td>
<td>Reduced need to maintain the entity structure</td>
<td>Reduced role owner administration</td>
</tr>
<tr>
<td></td>
<td>Reduced reliance on HR</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Limitations</th>
<th>User Based Security</th>
<th>Position Based Security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Increased user administration maintenance / access creep</td>
<td>Maintenance of the entity structure</td>
</tr>
<tr>
<td></td>
<td>Increase in user security administration tasks</td>
<td>Increased reliance on HR for security tasks</td>
</tr>
<tr>
<td></td>
<td>Increased reliance on role owners</td>
<td>Reduced flexibility</td>
</tr>
<tr>
<td></td>
<td>Increase in compliance concerns</td>
<td></td>
</tr>
</tbody>
</table>

Source: Protiviti Australia
5.3 Table and Program Maintenance

Data maintenance is a critical control to provide assurance that information recorded, processed and reported remain complete, accurate and valid throughout the update and storage process. Managing data includes the controls and procedures used to support information integrity, including its completeness, accuracy, authorisation and validity. Generally, data management controls are designed to support initiating, recording, processing and reporting financial information.

Functional overview

The SAP system, in elementary terms, is a compilation of programs which interact with relational database tables. Users manipulate the data contained in these tables through the graphical user interface (GUI). Each table or program may relate to either configuration or transactional data.

Most tables and programs are standard functionality delivered by SAP; however, custom tables and programs are often used to optimise the system to an entity’s business processes. Development of these custom components is facilitated within the SAP development tools. The system’s integrity is extremely sensitive to these activities, which necessitates strict change control procedures.

Commonly identified control weaknesses

The following control weaknesses typically occur in performing table and program maintenance:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABAP reports</td>
<td>All ABAP reports that need to be executed should be attached to info system report trees. In order to totally secure ABAP programs from unauthorised use, all programs can be assigned to an authorisation group and access restricted via authorisation group using the authorisation object S_PROGRAM.</td>
</tr>
<tr>
<td>Custom programs</td>
<td>Any custom transactions or programs that are developed should follow a consistent naming standard which complies with SAP conventions. Custom transactions and programs should be developed with appropriate security included within them. Often, transaction code security is relied upon only to secure custom programs.</td>
</tr>
<tr>
<td>Access to data dictionary and to maintain tables</td>
<td>Access to maintain the SAP data dictionary and SAP tables using transactions SM30 must be restricted to key database administration staff members.</td>
</tr>
<tr>
<td>Data browser access</td>
<td>Data browsing transactions, such as SE16, are often incorrectly allocated to a large number of users. SE16 can be used to view sensitive data, including executive payroll details.</td>
</tr>
</tbody>
</table>
Significant risks

High
- Changes to critical database tables are not logged
- Users have the ability to modify development programs in production
- Inappropriate access to the data dictionary

Medium
- Tables and programs are not restricted by authorisation group

Risks and controls

**R515: Changes to critical database tables are not logged**

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Changes to critical database tables are not logged.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
</tbody>
</table>

**Establishing table logging**
SAP provides the ability to log changes to critical tables. This capability should be established for critical tables. It should be recognised that establishing logging can impact system performance; the number of tables that are logged must be restricted. To establish table logging, the system profile parameter rec/client needs to be activated. The individual tables that are to be logged must also be set in transaction SE13. (C875)

**Manual controls**

**Logging, review and follow up of changes to critical tables**
Changes to critical tables like Clients (T000); Company Codes (T001); Fiscal Periods for Company Codes (T001B); and Foreign Currency Exchange Rates (TCURR) should be logged, reviewed, and adequately followed up. (C856)

---

**Logging changes to critical tables**

An entity had to adjust their financial statements after month end because a custom table had been incorrectly changed, resulting in the failure to settle a significant cost to the General Ledger.

The entity had failed to enable table logging on this custom table; therefore, they were not able to determine who had incorrectly changed the table.

Source: Protiviti Australia
### R516: Users have the ability to modify programs in production

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Inappropriate modification of production programs could lead to system instability and/or loss of data integrity.</td>
</tr>
</tbody>
</table>
| Controls | **Removing developer keys from the production environment**  
The ability to create or change a program in SAP is controlled by the allocation of developer keys. Without a developer key, SAP programs cannot be maintained. Ideally, developer key access should be removed from the production environment. The risk of allocating a developer key in production is increased if the client settings allow modification of programs in production. If it is impossible to change production programs, then even with a developer key, a user cannot not update a SAP program in production. (C1091) |

### R517: Inappropriate access to the data dictionary

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Inappropriate access to the data dictionary could result in unauthorised changes to database tables, resulting in data integrity issues.</td>
</tr>
</tbody>
</table>
| Controls | **Configuration controls**  
**Restricted access to the data dictionary**  
Access to maintain the SAP data dictionary must be restricted to key database administration staff members. (C854) |

### R518: Tables and programs are not restricted by authorisation group

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Unauthorised access may be gained to a program in the production environment to custom tables if they have not been assigned an authorisation group.</td>
</tr>
</tbody>
</table>
| Controls | **Configuration controls**  
**Assigning an authorisation group and restricting access to custom tables**  
Custom tables should be assigned an authorisation group and access should be restricted through authorisation object S_TABU_DIS. Authorisation groups should be assigned to production programs to prevent modification. (C833) |
Security considerations

• Users should be restricted from executing ABAP programs in the production environment. There are many powerful ABAP programs in the system that perform sensitive functions (i.e. deleting master data) yet do not incorporate any security checks. Access to the transactions used to nominate then execute ABAP programs, including FGRP Report painter should be restricted.

• Access to development functions, including the ability to maintain ABAP programs, should be totally restricted in the production environment. This is controlled via the authorisation object S_DEVELOP – ABAP Workbench which, apart from display access, should not be allocated in production.

• SAP has functionality to allow a user to perform operating system (OS) commands from within SAP using a system power user in the OS. Access to these utilities should be restricted from all users in the production environment (i.e. transaction SM69; authorisation object S_BDC_MONI with a value REOG). Operating system access should be administered via the operating system itself and not from within SAP.

• Specific transactions that allow direct updating of tables (i.e. SE16, SM30) exist. Access to such transactions must be restricted to authorised users through the authorisation object S_TABU_DIS – Table maintenance.

• Some tables are client-independent. This means that if these tables are updated in one client, all SAP clients in the same environment (system) are affected. Access to maintain client-independent tables for non production clients, which reside on the production client machine, must be restricted. This is provided by the authorisation object S_TABU_CLI – Cross-client Table Maintenance.

• All system tables are delivered with a ‘table class’ assigned. All users with table maintenance responsibilities should be restricted to the appropriate table class, and extreme care should be taken when assigning access to maintain tables in the class &NC& – W/o auth group (tables that are not assigned a specific class). Access to display tables should also be restricted, as many tables contain sensitive information (i.e. HR tables). This access should be restricted by table class.

• Access to data dictionary (system tables) transactions (i.e. SE11, SE13) should be adequately restricted in all clients in the production system. These transactions include the ability to maintain and display data dictionary tables, as well as maintaining technical settings and running utilities for system tables.
Key transaction codes and authorisation objects for table maintenance and programs

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td>Description</td>
</tr>
<tr>
<td>CMOD</td>
<td>Enhancements</td>
</tr>
<tr>
<td>SA38</td>
<td>ABAP Development</td>
</tr>
<tr>
<td>SD11</td>
<td>Data Modeller</td>
</tr>
<tr>
<td>SE11, SE13, SE14, SE15</td>
<td>ABAP Dictionary Utilities</td>
</tr>
<tr>
<td>SE16</td>
<td>Data Browser</td>
</tr>
<tr>
<td>SE37, SE38</td>
<td>ABAP Function Modules and Editor</td>
</tr>
<tr>
<td>SE93</td>
<td>Maintain Transaction Codes</td>
</tr>
<tr>
<td>SM30, SM31</td>
<td>Call View Maintenance (Tables)</td>
</tr>
<tr>
<td>SNR0</td>
<td>Maintain Number Ranges</td>
</tr>
<tr>
<td>SPRO</td>
<td>Customising: Edit Project (IMG Config)</td>
</tr>
<tr>
<td>SQ01</td>
<td>SAP Query: Maintain Queries</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>S_Develop</td>
<td>ABAP Workbench (Development)</td>
</tr>
<tr>
<td>S_Number</td>
<td>Number Range Maintenance</td>
</tr>
<tr>
<td>S_Program</td>
<td>ABAP: Program run checks</td>
</tr>
<tr>
<td>S_Project</td>
<td>Project Management: Project authorisation</td>
</tr>
<tr>
<td>S_Query</td>
<td>Authorisation for SAP Query</td>
</tr>
<tr>
<td>S_Tabu_CLI</td>
<td>Cross-client Table Maintenance</td>
</tr>
<tr>
<td>S_Tabu_Dis</td>
<td>Table Maintenance (via standard tools such as SM30)</td>
</tr>
</tbody>
</table>
Optimising the SAP control environment

Better practice items to consider in the maintenance of production database tables and programs include:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security policies</td>
<td>Adequate security guidelines should be in place to ensure that users and IT staff are prevented from accessing programs and data. This security policy should be enforced by appropriate security settings across all IT environments (database management system, operating system and local area network). A consistent security policy should be adopted across all environments.</td>
</tr>
<tr>
<td>Emergency access</td>
<td>There should be clearly defined emergency access procedures for the production SAP system. This should include monitoring of all activity performed while emergency access is granted to ensure that unauthorised or incorrect changes to data or programs are detected.</td>
</tr>
<tr>
<td>Sensitive system tables</td>
<td>Changes to sensitive system customising tables (including CTS tables) should be logged in both the development and production environments and the report Analysis of table log database reviewed on a regular basis to ensure that any unauthorised table changes are detected.</td>
</tr>
<tr>
<td>Restricting access to sensitive tables</td>
<td>Access to sensitive tables including payroll tables that hold executive pay rate details should be restricted using authorisation object S_TABU_DIS.</td>
</tr>
</tbody>
</table>
5.4 Basis System Administration

SAP administration is critical in ensuring that a reliable application system is maintained, and supports the business processes to initiate, record, process and report financial information. Deficiencies in this area could significantly impact an entity’s financial reporting. For instance, lapses in the continuity of application systems may prevent an entity from recording financial transactions and thereby undermine its integrity.

SAP administration procedures should also include procedures such that security and processing integrity controls are set up in the system and maintained through its life cycle unauthorized system components.

Functional overview

The Basis component’s fundamental purpose is to serve as the functional module for System Administration. It provides the software required to configure, manage and maintain a healthy SAP operating environment. Basis System Administration broadly covers responsibilities for maintaining the client/server architecture and configuration, the relational database supporting SAP, the interfaces with other systems and elements, and general system and user parameters. In addition, system administrators are able to utilise the Computing Centre Management System (CCMS) for monitoring system performance.

A typical SAP system will have a team that is responsible for system administration. Appropriate procedures should to be implemented to ensure that the system administration responsibilities are well controlled and protect the integrity of system data.

Commonly identified control weaknesses

The following control weaknesses typically occur in performance of system administration tasks:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production company codes</td>
<td>Entities rarely set production company codes to ‘productive’. The productive indicator prevents data within the company code from being deleted by certain SAP programs which are primarily used during the test phase of an SAP implementation project.</td>
</tr>
<tr>
<td>Cross-client objects</td>
<td>Entities rarely restrict the ability to change cross-client objects in the production client. All customising should be performed and tested in other systems before transport to the production system.</td>
</tr>
<tr>
<td>Failure to lock sensitive and unused transactions</td>
<td>There are key transaction codes, such as SCC4, that allow users to delete the SAP client. It is rare that these transactions are locked from use.</td>
</tr>
</tbody>
</table>
**Significant risks**

- **High**
  - SAP security authorisation checks are turned off
  - SAP database is not properly maintained

- **Medium**
  - Inadequate user and system documentation
  - Client, country and company code configuration is inadequate
  - SAProuter settings are incorrect

**Risks and controls**

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>R519: SAP security authorisation checks are turned off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk rating</td>
<td>HIGH</td>
</tr>
<tr>
<td>Risk description</td>
<td>It is possible to globally turn off the operation of specific authorisation objects which control access to SAP transactions. This is a significant risk as it essentially could be used to effectively eliminate important elements of the SAP security architecture.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td>Authorisation checks enabling</td>
</tr>
<tr>
<td></td>
<td>It is only possible to deactivate authorisation checks if the Auth/Object_Disabling_Active system parameter is set to ‘Yes’.</td>
</tr>
<tr>
<td></td>
<td>Globally disabling authorisation checks should not be allowed, as its intent can often have far-reaching and unintended implications in the system.</td>
</tr>
<tr>
<td></td>
<td>Therefore, this parameter should be set to ‘No’ to prevent the practice of object disabling. (C695)</td>
</tr>
</tbody>
</table>
### R520: SAP database is not properly maintained

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>The SAP database may lose its integrity due to misuse, unauthorised changes, or fraud. In addition, if not monitored appropriately, the database may run out of space, forcing the system to shut down.</td>
</tr>
</tbody>
</table>

### Controls

**Configuration controls**

1. **Tasks to administer the database running SAP**
   Responsibility should be allocated to administer the database running SAP.
   Key tasks that should be performed include:
   - Maintenance of the data dictionary;
   - Liaising with users and assigning responsibilities for ownership of data elements;
   - Monitoring database performance;
   - Ensuring database integrity; and
   - Establishing restart/recovery procedures. (C667)

2. **Manual expansion of database tables**
   SAP database tables must be expanded manually to allow further input of data. If this is not performed, the SAP system will reject new data until the system is shutdown completely and the table is expanded manually. It is, therefore, important to monitor space available for database tables. This can be performed through a variety of utilities, including the SAP alert monitor. (C664)
R521: Inadequate user and system documentation

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>SAP user and system documentation does not adequately document the SAP environment. This can cause problems if SAP programs and configuration is lost or key users leave the entity; business processes depending on the efficiency and effectiveness of the SAP system may be negatively impacted or even ground to a halt, affecting an entity’s ability to achieve its objectives.</td>
</tr>
</tbody>
</table>
| Controls        | Manual controls

Existence of user and system documentation
Both user and system documentation should be created for the SAP system. Documentation should include:
- Business policies and user documentation:
- Business policies;
- Outline of key business processes;
- User documentation; and
- Training material.
- System documentation
- Documentation of IMG configuration settings;
- Interface schema;
- Process maps; and
- Program documentation for client customisations. (C1092)
R522: Client, country and company code configuration is inadequate

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>To ensure that SAP functions correctly, it is important that client, country and company code settings are appropriate. Inappropriate settings may impact the integrity of financial records, or cause a disruption to the SAP system.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>Appropriate configuration of country settings</strong></td>
</tr>
<tr>
<td></td>
<td>Country settings can have a significant impact on key risk areas. Inappropriately configured country settings can result in inaccuracies in financial records. The following configuration items must be considered:</td>
</tr>
<tr>
<td></td>
<td>• Procedure – specifies the conditions that are allowed for a document and defines the sequence in which they are used.</td>
</tr>
<tr>
<td></td>
<td>• Currency – determines the currency that is used throughout the SAP system.</td>
</tr>
<tr>
<td></td>
<td>• Discount base net – indicates that tax on sales/purchases is not included in the base amount used for calculating cash discounts.</td>
</tr>
<tr>
<td></td>
<td>• Tax base net – indicates that the cash discount is deducted from the base amount used for calculating taxes on sales/purchases. (C689)</td>
</tr>
<tr>
<td></td>
<td><strong>Defining of production client</strong></td>
</tr>
<tr>
<td></td>
<td>It is important that the production client is defined as a production client in the SAP IMG. This ensures that SAP will not allow perform any remote copies into the SAP production system. (C784)</td>
</tr>
</tbody>
</table>

R523: SAProuter settings are incorrect

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>SAProuter settings are incorrect, resulting in system inoperability.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>Restricted access to SAProuter settings</strong></td>
</tr>
<tr>
<td></td>
<td>The SAProuter is a program that functions as an intermediate station between SAP systems or programs. SAProuter functions as an application level gateway (proxy) that enables and regulates access to SAP through the SAProuter port. SAProuter allows a connection to a SAP system without a direct network connection between the client computer and the application server. Access to SAProuter settings must be properly configured and restricted. (C858)</td>
</tr>
</tbody>
</table>
Security considerations

- Access to the S_RZL_ADM – CCMS: System Administration authorisation object should be restricted, as this provides users with access to powerful systems administration functions, including:
  - Creating new clients;
  - Locking / unlocking transactions;
  - Controlling spool (print) requests; and
  - Deleting data without archiving.

- Access to the batch processing and spool control authorisation objects should be restricted, as these provide access to administration functions. These functions should be restricted to the following authorised users:
  - S_BTCH_ADM – Batch admin
  - S_BTCH_JOB – Delete background jobs of other users.
  - S_SKOM_SRV – Server authorisation.
  - S_SPO_ACT
    - Change attributes of protected spool request.
    - Redirect output to a different printer.
    - Delete request manually.
### Key transaction codes and authorisation objects for System Administration

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transactions</strong></td>
<td></td>
</tr>
<tr>
<td>OBR3</td>
<td>C FI Maintain Table T001</td>
</tr>
<tr>
<td>RZ04</td>
<td>Maintain SAP Instances</td>
</tr>
<tr>
<td>RZ06</td>
<td>Alerts Thresholds Maintenance</td>
</tr>
<tr>
<td>RZ10</td>
<td>Maintenance of Profile Parameters</td>
</tr>
<tr>
<td>SCC1, SCC4, SCC5, SCC7, SCC8, SCC9, SCCCL</td>
<td>Client Administration Functions</td>
</tr>
<tr>
<td>SCC4</td>
<td>Client Maintenance</td>
</tr>
<tr>
<td>SE11</td>
<td>ABAP dictionary</td>
</tr>
<tr>
<td>SE80</td>
<td>Object Navigator</td>
</tr>
<tr>
<td>SE81</td>
<td>Application Hierarchy</td>
</tr>
<tr>
<td>SM01</td>
<td>Lock Transactions</td>
</tr>
<tr>
<td>SM12</td>
<td>Display and Delete Locks</td>
</tr>
<tr>
<td>SM49</td>
<td>Execute external OS commands</td>
</tr>
<tr>
<td>SM51</td>
<td>List of SAP Systems</td>
</tr>
<tr>
<td>SM59</td>
<td>RFC Destinations (Display/Maintain)</td>
</tr>
<tr>
<td>SM69</td>
<td>Maintain External OS Commands</td>
</tr>
<tr>
<td>SPAD</td>
<td>Spool Administration</td>
</tr>
<tr>
<td>SPRO</td>
<td>Customising Project</td>
</tr>
<tr>
<td><strong>Authorisation Objects</strong></td>
<td></td>
</tr>
<tr>
<td>S_ADMI_FCD</td>
<td>Basis Administrative System Authorisations</td>
</tr>
<tr>
<td>S_BTCH_ADM</td>
<td>Background Processing: Background Administrator</td>
</tr>
<tr>
<td>S_CLNT_IMP</td>
<td>Data Import for Client Copy</td>
</tr>
<tr>
<td>S_DEVELOP</td>
<td>ABAP Workbench (Development)</td>
</tr>
<tr>
<td>S_RZL_ADM</td>
<td>CCMS: System Administration</td>
</tr>
<tr>
<td>S_TABU_DIS</td>
<td>Table Maintenance (via standard tools such as SM30)</td>
</tr>
</tbody>
</table>
### Optimising the SAP control environment

**Optimising SAP controls**

- Unused transactions
- Segregation of duties

Better practice items to consider in the performance of system administration tasks include:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unused transactions</td>
<td>If transactions are not required by an entity, such transactions should be locked from use in table TSTC using transaction SM01. It is also important to restrict the ability of users to unlock sensitive transactions. As a result, access to the SM01 transaction should be properly restricted to system administrators.</td>
</tr>
<tr>
<td>Segregation of duties</td>
<td>It is considered best practice to separate the Security Administration and the System Administration functions. Both of these roles have a significant degree of inherent risk to system integrity, however, an employee granted the ability to fulfil both responsibilities would have limitless capabilities within the system. Ideally, the roles of developer, transport administration, system administration, and security administration should be segregated to prevent integrity issues. Due to size of entities and limited resource budgets, many entities will have to settle for a segregation of security and Basis responsibilities.</td>
</tr>
</tbody>
</table>
5.5 Mass Maintenance

Functional overview

Mass Maintenance functionality has been developed as an effective tool to maintain large amounts of data. For example, the Mass Maintenance function allows a user to change data in a large number of purchase orders or requisitions through the execution of a single transaction.

Mass Maintenance functions are supported for a number of documents, including:

- Material master;
- General ledger records;
- Purchasing info records;
- Vendor and customer master;
- Purchase orders and purchase requisitions; and
- User master records.

Commonly identified control weaknesses

Control risks relevant to mass maintenance include:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inappropriate access to mass maintenance capabilities</td>
<td>Clients often allocate inappropriate access to Mass Maintenance transactions increasing the risk of the processing of inappropriate changes to master records and transaction data.</td>
</tr>
<tr>
<td>Incorrect changes to master data using Mass Maintenance capabilities</td>
<td>Typical master data integrity controls such as subsequent review of changes to sensitive fields are rarely applied when using the Mass Maintenance function.</td>
</tr>
</tbody>
</table>

Significant risks

- Inappropriate or unauthorised changes made to data
## Risks and controls

### R524: Inappropriate or unauthorised changes made to data

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>While using Mass Maintenance functionalities, a user may mistakenly or fraudulently change a significant amount of data in the system, leading to a material lack of integrity in system data and/or fraudulent transactions. Inappropriate use of Mass Maintenance functionality could severely harm system performance, leading to a slowdown or disruption in performing other SAP related tasks.</td>
</tr>
</tbody>
</table>

### Controls

#### Configuration controls

**Restricted access to security authorisations for mass maintenance**

Granting security authorisations for mass maintenance functionality needs to be restricted to appropriate personnel. These functions are meant to be used only occasionally for a major event (i.e. a customer moved locations and all open orders must be delivered to the new address). Users granted the ability to perform mass maintenance are required to attend training on the use of the maintenance functionality. (C1093)

#### Manual controls

1. **Procedures for mass changes**

   Procedures which require all mass changes to be pre-approved should be put in place. Standard SAP reports should be used to monitor and reconcile all master data changes. (C1094)

2. **Review of changes**

   Changes are typically documented in a spreadsheet before being uploaded. It is important that are changes are reviewed for completeness, accuracy and for any duplicate records before being uploaded. (C1095)
Security considerations

Due to the increased risk associated with providing a user with the ability to maintain and change large amounts of data simultaneously, access to the following key transactions should be restricted to key experienced staff with authority to make changes:

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Area</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>FMMI</td>
<td>Mass Maintenance of Open Intervals</td>
</tr>
<tr>
<td>IMAM</td>
<td>Mass Maintenance of Aprop Requests</td>
</tr>
<tr>
<td>KE55</td>
<td>Mass Maintenance of Profit Centre</td>
</tr>
<tr>
<td>KE56,KE57</td>
<td>Mass Maintenance C-Code Assgnt</td>
</tr>
<tr>
<td>MASSOBJ</td>
<td>Mass Maintenance Objects</td>
</tr>
<tr>
<td>MM17</td>
<td>Mass Maintenance (Ind Mat Master)</td>
</tr>
<tr>
<td>MM46</td>
<td>Mass Maintenance (Retail)</td>
</tr>
<tr>
<td>MSJ1</td>
<td>Mass Maintenance (background)</td>
</tr>
<tr>
<td>MSL1</td>
<td>Mass Maintenance Logs</td>
</tr>
<tr>
<td>MSL2</td>
<td>Delete Mass Maintenance Logs</td>
</tr>
<tr>
<td>OB_GLACC11, OB_GLACC12, OB_GLACC13</td>
<td>GL master records mass maintenance</td>
</tr>
<tr>
<td>QI05, QI06</td>
<td>Mass Maintenance QM procurement keys</td>
</tr>
<tr>
<td>SOY1</td>
<td>Mass Maintenance of Users</td>
</tr>
<tr>
<td>SU10</td>
<td>User Mass Maintenance</td>
</tr>
<tr>
<td>WB30</td>
<td>Mass Maintenance MG to plant</td>
</tr>
<tr>
<td>WTAD_VKHM_MAINTAIN</td>
<td>Mass Maintenance (Material Additions)</td>
</tr>
<tr>
<td>XD99</td>
<td>Customer Mass Maintenance</td>
</tr>
<tr>
<td>XK99</td>
<td>Vendor Mass Maintenance</td>
</tr>
<tr>
<td><strong>Authorisation Objects</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>B_MASSMAIN</td>
<td>Cross-Application Mass Maintenance Tool</td>
</tr>
</tbody>
</table>
Optimising the SAP control environment

Better practice items to consider in the use of Mass Maintenance capabilities include:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mass Maintenance procedures</td>
<td>Using mass maintenance transactions can be a very powerful tool for master data in the system, however, this functionality could also be used to either unintentionally or intentionally wreak havoc on the system. It is extremely important for an entity to put in place procedures for the use of all mass maintenance functions. These procedures should require pre-approval for all mass changes. Management should monitor the usage of these transactions, as well as reconcile all master data changes on a frequent basis.</td>
</tr>
</tbody>
</table>
5.6 NetWeaver Security

Functional overview

SAP NetWeaver comprises several technologies and components: a portal framework, business intelligence and reporting, Business Process Management (BPM), integration, Master Data Management (MDM), a common run-time application server, and the SAP application development and management platform. NetWeaver is a Java based platform and provides an open based architecture which enables system linkage and interfaces with other SAP and non-SAP systems.

Configuration and changes to the various services are performed via the SAP NetWeaver Administrator (NWA), which is the central point for the administration, configuration, and monitoring for the various SAP and non SAP components that are managed by the NetWeaver.

This chapter of the guide focuses on security risks associated with NetWeaver. Configuration and associated configuration risks are outside of this guide’s scope.

Security considerations

Given the potential impact to processing, data and infrastructure, there is a need to ensure that security considerations of NetWeaver are addressed to ensure a secure environment.

The following outlines key security risks that have to be considered in implementing NetWeaver:

1. To ensure secure network connections to and from the SAP Web Application server, use Secure Sockets Layer (SSL) protocol encryption. SSL will provide:
   - Server-side authentication
   - Client side authentication
   - Mutual authentication
   - Data encryption

2. SAP NetWeaver security has been configured to allow encryption/signature based on XML for authentication and non-repudiation. The following Web Service Security parameters must be appropriately configured:
   - Http destination type (G)
   - Signature processing logical port for proxy class CO_WSSEWSSPROCESSOR_VI_DOCUMENT
   - Web service definition with Basic authorisation: SOAP Pro
   - Authentication Certificate generated in J2EE and uploaded into the ABAP stack
   - Web service security profile (WSSPROFILE)
   - The web service security profile assignment to the web service in Visual Administrator
   - Deployable Proxy project in Developer Studio
• Authentication options set to Encryption + XML Signature
• J2EE role assignment to web service for permission check

3. Access to key authorisation objects should be restricted. Key objects include:

• S_SERVICE for each web service  
• S_TCODE restricted to WSSADMIN  
• S_DEVELOP restricted to display only

4. Access to Restrict User Management Engine (UME) roles must be adequately restricted. UME Roles are essentially a collection of Java permissions and actions. Note – these permissions and actions are not ‘visible’ to users via the UME.

User Authentication and Management in NetWeaver is performed via the User Management Engine (UME) and the Visual Administrator (for SAP J2EE). In addition to these, where the NetWeaver installation is used in conjunction with ABAP for user management, the standard SAP user management functions would still be valid (SU01, PFCC, CUA).

Permissions and roles for UME roles are outlined within the UMErole.xml file. Checks should be performed to ensure that this file has not been modified from the point of installation.

The following actions/permissions are contained within the UMErole.xml file. A review of the roles that contain these actions permissions, as well as the users assigned to those particular roles, should be performed to ensure the appropriateness of access.

<table>
<thead>
<tr>
<th>UME actions/permissions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UME.AclSUperUser</td>
<td>Super User permission</td>
</tr>
<tr>
<td>Ume.Manage_all</td>
<td>User Administrator permission</td>
</tr>
<tr>
<td>UME.Manage_All_User_passwords</td>
<td>User Administrator permission</td>
</tr>
<tr>
<td>Ume.Manage_Users</td>
<td>User Administrator permission</td>
</tr>
</tbody>
</table>

Access to the following Visual Administrator and UME roles should be restricted:

<table>
<thead>
<tr>
<th>UME/Visual Administrator Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Security role that provides all access to the J2EE engine</td>
</tr>
<tr>
<td>Administrator</td>
<td>Security role that provides unrestricted administrative permissions over the applications and services on the J2EE environment.</td>
</tr>
</tbody>
</table>
Access to the following J2EE permissions should be restricted to authorised personnel only:

<table>
<thead>
<tr>
<th>Visual Administrator Role/Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet_login</td>
<td>Telnet Administrator Role for the J2EE engine. Access via the Shell Console Administrator tool at WebDynpro.</td>
</tr>
<tr>
<td>$SAP_J2EE_ENGIN/upload</td>
<td>Ability to upload permissions to the J2EE environment.</td>
</tr>
<tr>
<td>$SAP_JAVA_NWADMIN_CENTRAL</td>
<td>Administrator Role. The ability to make changes via the NWA utility. This role enables management of the entire System LandscapeDirectory (SLD). The SLD defines each SAP system.</td>
</tr>
<tr>
<td>$SAP_JAVA_NWADMIN_LOCAL</td>
<td>Administrator Role. The ability to make changes via the NWA utility. This role enables changes to the local system only which NWA runs from.</td>
</tr>
</tbody>
</table>

Other Security Considerations for NetWeaver would include the following. (Note these are not generic and need to be considered on a case-by-case basis):

- Security Considerations for the Java Message Service of the J2EE engine
  - Communication/interface security could potentially become an issue if the SAP environment is interfaced with external applications. Security considerations here would include firewall settings, router settings and other necessary communication and data transmission security settings.

- Java Virtual Machine Security
  - Patch Management is a key component of security at this level. This is required to guard against malicious code and other viruses.

- Database (Jco) Connection Security
  - Security considerations relating to the various database connections that are performed at the NetWeaver level. Access to these databases would need to be created and configured at the NetWeaver layer to enable the J2EE connections. Data stored at the NetWeaver level is encrypted.
5.7 Central User Administration

Functional overview

Central User Administration (CUA) allows all user administration activities to be performed from a central system. CUA allows security administrators to centrally maintain a user master record and assign the appropriate access for several systems.

Though not covered in this guide, it is worth noting that in recent years, third party and SAP-proprietary Identity Management (IDM) tools have become more prevalent in the market. IDM solutions take the CUA concept one step further in maintaining one central identity for each employee across all the software and security systems of an entity. These tools allow for a more secure, single identity environment.

In addition, the SAP GRC Access Control toolset discussed in the Chapter 5 Feature article provide a Compliant User Provisioning tool which could potentially replace the traditional CUA system.

Significant risks

- CUA configuration and ALE landscape may not be configured correctly

Risks and controls

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>Risk description</th>
<th>Controls</th>
</tr>
</thead>
</table>
| MEDIUM      | CUA configuration and ALE (Application Linking and Enabling) landscape may not be configured correctly, resulting in the failure of systems to interface effectively. Access to CUA or ALE functions may not be adequately secured, resulting in unauthorised changes to user’s access rights. | Configuration controls

Defining of CUA configuration parameters
The CUA system operates off its own instance and set of configuration parameters. Appropriate configuration parameters, particularly within the Basis area similar to those of the SAP ERP system, need to be defined for CUA. (C1096)

Restricted access to CUA and the ALE landscape
Access to CUA and the ALE landscape should be restricted to key authorised personnel. (C1097)
Security considerations

Access to the configuration of CUA transactions must be controlled. Consideration should be given to restricting access to relevant user administration staff to the CUA maintenance transactions in the table below. In addition, all user administration security and segregation of duties concerns need to be enforced across relevant systems (i.e. User Administration in CUA and System Administration in SAP ERP is a segregation of duties conflict).

CUA maintenance transactions that require restricted access

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td>Description</td>
</tr>
<tr>
<td>SALE</td>
<td>Display ALE Customising</td>
</tr>
<tr>
<td>SCUA, SCUM</td>
<td>Central User Administration</td>
</tr>
<tr>
<td>SCUL</td>
<td>Central User Management Log</td>
</tr>
<tr>
<td>SUGR</td>
<td>Maintain User Groups</td>
</tr>
<tr>
<td>SCUG</td>
<td>Transfer Users</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>S_USER_SYS</td>
<td>User Master Maintenance: System for Central User Maintenance</td>
</tr>
<tr>
<td>S_USER*</td>
<td>All other user maintenance objects still apply</td>
</tr>
</tbody>
</table>
Functional overview

The backup and recovery process is an essential process for every entity. In the unfortunate event of a disaster or system malfunction, an entity needs to ensure that their data is secure and can be recovered. The loss of the configuration and transactional data from SAP would cause devastating consequences to an entity, from which it may not recover or recover fully from.

SAP data is stored in a relational database structure. A data backup consists of database files and SAP files (i.e. programs, log files) which are stored in a central directory. The Basis administrator must use operating system tools to back up this directory tree, which is part of the hierarchical file system. Since it is generally very dynamic, SAP data requires a comprehensive security strategy for data retention.

With the evolution of the SAP landscape now including multiple components operating on individual platforms, the backup and recovery procedures for an entity must be revaluated periodically to ensure that the recovery procedures provide cover for all critical systems. In addition to the base SAP ERP system, the Java environments running on the NetWeaver platform must be considered.

Significant risks

- Critical SAP data is lost
### Risks and controls

**R526: Critical SAP data is lost**

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Backup and recovery procedures are inadequate and/or incomplete, resulting in critical SAP data not being recovered in the event of a disaster.</td>
</tr>
<tr>
<td>Controls</td>
<td><strong>Manual controls</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Documented and operating backup strategy</strong></td>
</tr>
<tr>
<td></td>
<td>A backup strategy should be clearly documented and operating to ensure that SAP programs and data are adequately backed up. The strategy should include:</td>
</tr>
<tr>
<td></td>
<td>• An outline of the entire backup process;</td>
</tr>
<tr>
<td></td>
<td>• A schedule for full and incremental backups performed on a daily basis;</td>
</tr>
<tr>
<td></td>
<td>• A retention period of at least 28 days (4 weeks);</td>
</tr>
<tr>
<td></td>
<td>• A minimum of 10 generations of complete database backups; and</td>
</tr>
<tr>
<td></td>
<td>• A data rotation process for storing backup media off-site for maximum effectiveness. (C633)</td>
</tr>
<tr>
<td></td>
<td><strong>Regular testing of backup and recovery procedures</strong></td>
</tr>
<tr>
<td></td>
<td>Backup and recovery procedures should be tested regularly to ensure compliance with the procedures and to make any improvements considered necessary. (C1098)</td>
</tr>
<tr>
<td></td>
<td><strong>Development of disaster recovery and business continuity plans</strong></td>
</tr>
<tr>
<td></td>
<td>A comprehensive disaster recovery plan and business continuity plan should be developed to ensure that the entity can continue to operate in the event of a disaster. These plans should include, but not be limited to covering, the IT systems. (C1099)</td>
</tr>
</tbody>
</table>
5.9 Portal Security (SAP Enterprise Portal)

Functional overview

SAP Enterprise Portal provides users with a single point of access to all applications, information, and services needed to accomplish their daily tasks. Links to ‘back-end’ and legacy applications, self-service applications, company intranet services and internet services are all readily available in the user’s portal. Because the borders between company intranets and the internet are blurring, comprehensive security is vital to protect the company’s business.

This section of the guide does not seek to describe the key risks and capabilities of the SAP Portal; rather, illustrates that, in terms of the security environment, the Portal supports authentication of users. Once users are granted access to the Portal and access a SAP functional item, normal SAP transaction and authorisation security prevails.

For example, if a user is provided access to Employee Self Service through the Portal, the user will still require SAP ESS transaction codes and authorisation objects to be able to perform ESS functions.

Security considerations

The key security element controlled by the Portal is providing authentication for user access. Authentication provides a way of verifying the user’s identity before he or she is granted access to the Portal. Once the user has been authenticated, the user is issued a SAP logon ticket that allows them to access all the applications, information and services in SAP.

In the Portal, authentication is defined using authentication schemes which are assigned to iViews. Users log on to the Portal with a specific authentication scheme and this is stored in the user’s logon ticket. If a user needs to access an iView which requires a stronger authentication scheme, he or she must re-authenticate as specified by the stronger authentication scheme.

An authentication scheme is a definition of what is required for an authentication process. This includes:

- Type of information used to compute a user’s identity. For example, user ID and password and client certificate.
- How user data is checked. For example, against a LDAP directory or a SAP System.
- Validity of user logon, that is, the amount of time after which a user has to logon again.
- Priority, allowing authentication schemas to be ordered.

When using the Portal to allocate a SAP ERP or SRM function, normal SAP transaction and authorisation object security prevails.
Chapter 5 – Feature article

**GRC Access Control**

Overview 175
Risk Analysis and Remediation 176
Superuser Privilege Management 186
Overview

SAP user security is inherently complex to implement and to maintain. Ongoing monitoring of access controls is required to ensure that controls remain effective in mitigating access and security risks.

This Feature article provides an overview of the Governance, Risk and Compliance (GRC) Access Control module, which is a SAP solution to assist with implementing and monitoring SAP system controls. It provides an overview of risks and controls associated with two elements of the SAP GRC component: the Risk Analysis and Remediation Product (RAR) and Superuser Privilege Management, known as Firefighter (FF). RAR is an important toolset in mitigating segregation of duties risks, and FF provides functionality important for managing superuser or privileged access to SAP functions.

While this Feature Article describes risks and controls specific to GRC and FF implementation, many of the risks and control practices could be adapted to other similar tools or processes.

Implementing effective user access controls requires careful planning and analysis to ensure that reporting and monitoring tools, such as GRC, are correctly designed and implemented, thereby providing useful and accurate information for analysis and remediation of access risks.

What is GRC Access Control?

SAP GRC Access Control allows entities to automate, document, detect, remediate, mitigate, and prevent access and authorisation risks, including the management of segregation of duties and sensitive access risks.

The diagram below outlines the components of GRC Access Control.

GRC Access Control

- **Risk Analysis and Remediation**: detect, remove and prevent access and authorisation risk by preventing security and control violations before they occur.
- **Enterprise Role Management**: standardises and centralises role creation and maintenance.
- **Compliant User Provisioning**: automates provisioning, tests for segregation of duties risks and streamlines approvals to the appropriate business approvers.
- **Superuser Privilege Management**: enables users to perform emergency activities outside their role as a ‘privileged user’ in a controlled and auditable environment.
- **Continuous Access Management**: automates, document, detect, remediate, mitigate, and prevent access and authorisation risk.
- **Effective Management Oversight and Audit**: Focus on remaining challenges during recurring audits.

This feature article focuses on the Risk Analysis and Remediation and the Superuser Privilege Management components of the GRC Access Control solution.
Risk Analysis and Remediation

Risk Analysis and Remediation (RAR) is an automated security audit and segregation of duties analysis application that is used to identify, analyse, and resolve segregation of duties and security audit issues. A risk analysis to identify risks associated with a user, role, profile, or human resources (HR) object is initially performed. Subsequently, mitigation controls for risks that cannot be eliminated are then defined. It is also possible to define monitors and approvers, assign them to specific controls, and create business units to help categorise mitigation controls.

RAR facilitates the implementation of a preventative segregation of duties framework. When new access or existing user access rights are to be altered, the simulation capabilities of the product can be used to assess the associated security risk. This applies to:

- New and changes to user access.
- New and changes to security roles.
- Changes to Human Resource objects (if position-based security is used).

The following diagram provides an outline of the Risk Analysis and Remediation product:

### SAP Risk Analysis and Remediation Product

1. Identify and Select Risks to manage
2. Build and Maintain Rules
3. Detect Authorisation Risk
4. RemEDIATE and Mitigate
5. Test and Report
6. Prevent

Source: Protiviti Australia, adapted from SAP information.
There are two different architectures for the RAR:

- Version 4 is internal within SAP, built with ABAP. Risk analysis and remediation activities can be performed directly within SAP.

- Versions 5.1, 5.2 and 5.3 have a Java based front end and use a backend connector for the SAP system. Additional server infrastructure is required for version 5.

There are several functions or components that require consideration when implementing the RAR module:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User access risk</td>
<td>A risk is an opportunity for physical loss, fraud, process disruption, or productivity loss that occurs when individuals exploit a specific condition. Functions are the main component of risks. When a Risk Analysis or a Simulation is run, reports are generated presenting different types of information. Reports detail risks or conflicts or the use of critical actions by the User, Role, Profile, or HR Object. The reports allow a system manager to identify access risks.</td>
</tr>
<tr>
<td>Rule Architect</td>
<td>In order to identify the risks produced in Risk Analysis reports, it is important to identify the combinations of actions and permissions that represent conflicts. In addition to Rules and Business Processes, Rule Architect is used to build and maintain tables for Critical Roles and Critical Profiles, as well as other tables.</td>
</tr>
<tr>
<td>Mitigation Controls</td>
<td>Once Risk Analysis has been run and has identified access control risks, it is important to then identify Users, Role, Profile, or Objects that will require periodic monitoring if the risk cannot be removed. Mitigation Controls enables controls to be linked with or associated with User Access Risks so that risks so that controls can be applied to Users, Roles, Profiles, or HR Objects identified to violate segregation of duty principles identified as part of the risk analysis.</td>
</tr>
<tr>
<td>Alerts</td>
<td>Alerts are generated for the following reasons:</td>
</tr>
<tr>
<td></td>
<td>• A critical action was executed.</td>
</tr>
<tr>
<td></td>
<td>• A conflicting action was executed.</td>
</tr>
<tr>
<td></td>
<td>• A Mitigation Report transaction was not run within the specified time period.</td>
</tr>
</tbody>
</table>
Commonly identified control weaknesses

The following control weaknesses typically occur in RAR implementations:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to install an effective ruleset</td>
<td>Configuring a GRC segregation of duties ruleset is complex. It requires assessment of risk items, inclusion of custom transactions and modification of authorisation object rules. This is often not performed effectively, resulting in the reporting of incorrect results.</td>
</tr>
<tr>
<td>Failure to incorporate preventative checking within security processes</td>
<td>RAR provides the ability to implement preventative segregation of duties checking when performing user and role security maintenance. When implementing RAR, limiting effort is placed on redesigning security processes to incorporate preventative segregation of duties checking. This reduces the effectiveness of the RAR product.</td>
</tr>
<tr>
<td>Inefficient security remediation processes</td>
<td>RAR is a reporting tool which highlights segregation of duties and critical access risks. The remediation process includes changing the SAP security structure, modifying employees' responsibilities and documenting mitigation controls.</td>
</tr>
<tr>
<td>Inappropriate reliance on mitigation controls</td>
<td>Often emphasis is placed on mitigation controls rather than fixing underlying security problems. Reliance on mitigation controls increases the cost of compliance. Documented mitigation controls often do not adequately address the underlying segregation of duties risk.</td>
</tr>
</tbody>
</table>

Significant risks

- **High**
  - Inadequate configuration of segregation of duties ruleset
  - Ineffective identification, documentation or over-reliance on mitigation controls
  - Failure to implement preventative segregation of duties checking

- **Medium**
  - Incorrect setup of overall configuration options
# Risks and controls

**R550: Inadequate configuration of segregation of duties ruleset**

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>HIGH</th>
</tr>
</thead>
</table>
| Risk description | Configuring a RAR segregation of duties ruleset is complex and requires assessment of risk items, inclusion of custom transactions and modification of authorisation object rules. This is often not performed effectively resulting in the reporting of incorrect results. Typical problems with RAR rulesets include:  
- Inclusion of incorrect segregation of duties risks, which do not adequately address the entity's risk profile.  
- Failure to adequately consider custom transaction codes.  
- Inclusion of transaction codes that do not constitute a segregation of duties risk.  
- Failure to adequately configure authorisation object criteria.  
These problems result in either of the following situations:  
- Identification of false negatives, where users are identified with segregation of duties concerns which do not exist.  
- False positives, where users with actual segregation of duties results are not identified by RAR. |
| Controls | Key success factors in developing the ruleset include (C1011):  
- Performance of a risk evaluation workshop with key elements of the business. The workshop will review default GRC ruleset and evaluate whether the risks are relevant for the entity. Additional risks would also be considered.  
- Review the criticality and risk descriptions for all applicable risks. Ensure the risk descriptions are relevant for the entity.  
- Review of all custom transactions and include custom transactions that affect segregation of duties or critical action risks.  
- Assess the adequacy of all transactions that will be included within the ruleset.  
Configuration controls  
- Review authorisation object settings. Consider whether there are custom object settings that should be included. (C1012) |

---

**Important Update**

---

**GRC Access Control**

**Feature article: GRC Access Control**
### R551: Ineffective identification, documentation or over-reliance on mitigation controls

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>HIGH</th>
</tr>
</thead>
</table>
| Risk description | Often, emphasis is placed on mitigation controls rather than fixing underlying security problems. Mitigation controls can be documented within RAR against risks, users or roles. Conflicts relating to risks that have documented mitigation controls can be excluded from segregation of duties results and reporting. Possible risks with relying on mitigation controls include:  
- Documented mitigation controls often do not adequately address the documented segregation of duties risk.  
- Mitigation controls documented in RAR may not be effectively executed on a timely basis.  
- Reliance on mitigation controls is inefficient and increases the cost of compliance. |
| Controls | Reliance on mitigation controls should only be performed if it is not possible to segregate business functions or fix the security structure.  

**Manual controls**  
*Mitigation controls should only be documented for individual users and not for security roles.* (C1013)  
Key items to consider when using mitigation controls include:  
- The mitigation control should cover the entire segregation of duties risk.  
  Effective mitigation controls are typically system based, including the review of system based reports.  
- All mitigation controls should be documented, approved and be operating effectively before being included against conflicts in RAR.  
- The effectiveness of operation of each mitigation control should be reviewed on a periodic basis. A validity date can be set on mitigation controls within RAR. The validity date should be initial set for six months after implementation and then be reset to 12 month intervals. |
R552: Failure to implement preventative segregation of duties checking

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>RAR provides the ability to implement preventative segregation of duties checking when performing user and role security maintenance. When implementing RAR, there is a risk that limited effort is placed in redesigning security processes to incorporate preventative segregation of duties checking. This reduces the effectiveness of the RAR product.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
</tbody>
</table>
| Security procedures | should be enhanced to ensure that simulations are performed in the following situations (C1014):  
  - Create user.  
  - Modify user.  
  - Create security role.  
  - Change security role.  
  - Password reset or unlock user. |

R553: Incorrect setup of overall configuration options

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>RAR overall configuration options are incorrectly set, resulting in incorrect or ineffective reporting.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td>The following table outlines the available configuration options within RAR, the default and recommended settings. Only the configuration options that impact on the control environment are listed. (C1015)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
<th>Default Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Analysis / Default Report Type for Risk Analysis</td>
<td>This option sets the default Report Type when running a Risk Analysis</td>
<td>Permission</td>
<td>Permission</td>
</tr>
<tr>
<td>Risk Analysis / Default Risk Level for Risk Analysis</td>
<td>This option sets the default Risk Level when running a Risk Analysis.</td>
<td>ALL</td>
<td>ALL</td>
</tr>
<tr>
<td>Risk Analysis / Default User Type for Risk Analysis</td>
<td>This option sets the default User Type included when running a Risk Analysis.</td>
<td>Dialog</td>
<td>Dialog</td>
</tr>
<tr>
<td>Risk Analysis / Default ruleset for risk analysis</td>
<td>This option sets the default RuleSet included when running a Risk Analysis.</td>
<td>Global Ruleset</td>
<td>Entity Specific Ruleset</td>
</tr>
</tbody>
</table>
### R553: Incorrect setup of overall configuration options (continued)

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description</th>
<th>Default Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Analysis / Exclude Locked Users</td>
<td>This option specifies whether or not Locked Users are excluded when running a Risk Analysis.</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Risk Analysis / Exclude Expired Users</td>
<td>This option specifies whether or not Expired Users are excluded when running a Risk Analysis.</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Risk Analysis / Exclude Mitigated Risks</td>
<td>This option specifies whether or not users with mitigation controls are excluded when running a Risk Analysis.</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Risk Analysis / Ignore Critical Roles &amp; Profiles</td>
<td>This option specifies whether or not Roles and Profiles maintained in the Critical Roles table and the Critical Profiles table are ignored when running a Risk Analysis. The default value is NO. Setting the value to YES ignores all Critical Roles and Profiles from user analysis.</td>
<td>NO</td>
<td>NO, Unless specific roles or profiles require exclusion from the results.</td>
</tr>
<tr>
<td>Risk Analysis / Show Composite Role in User Analysis</td>
<td>This option specifies whether or not to show composite role information in addition to default single role information in detailed report when doing user analysis</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Mitigation Controls / Default expiration time for mitigation controls (in days)</td>
<td>When assigning mitigation controls to a risk it is important to specify the validity period of the Control. If the “To Date” is left blank the value in this option is used to calculate the end date of the validity period.</td>
<td>365</td>
<td>365 (180 upon implementation, 365 thereafter)</td>
</tr>
<tr>
<td>Enable Risk Change Log</td>
<td>This option enables logging of Risk changes.</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>Enable Function Change Log</td>
<td>This option enables logging of Function changes.</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>
Implementing preventative controls to monitor segregation of duties risks

Entities spend significant time and effort to address their segregation of duties problems, only for the problems to reappear every six months when their Internal Audit group or external auditors perform an assessment of the effectiveness of access controls.

This issue may be addressed through use of automated security tools that can quickly analyse and report segregation of duties issues, thereby strengthening the segregation of duties checking process.

Key elements of this process include:

• When creating new security roles or changing security roles, the security tool may be used to identify whether additional segregation of duties issues will be introduced.
• When allocating roles to user accounts, the security tool may assist to identify whether the new roles will cause problems with segregation of duties.
• The security tool is also useful to document mitigation controls against security risks where it was not possible to effectively segregate user access.
• Weekly/periodic reporting to management provides regular assurance that the controls are operating effectively.

Source: Protiviti Australia

Security considerations

The following table outlines standard security roles are delivered within RAR:

Standard security roles delivered within RAR

<table>
<thead>
<tr>
<th>Role</th>
<th>GRC RAR Security Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Staff (Reporting Only)</td>
<td>Version 4 (R/3):</td>
</tr>
<tr>
<td></td>
<td>/VIRSA/Z_CC.Reporting</td>
</tr>
<tr>
<td></td>
<td>Version 5 (UME):</td>
</tr>
<tr>
<td></td>
<td>CC.ReportingView</td>
</tr>
<tr>
<td>Business Staff (Reporting and the ability to maintain mitigation controls)</td>
<td>Version 4 (R/3):</td>
</tr>
<tr>
<td></td>
<td>/VIRSA/Z_CC.Reporting</td>
</tr>
<tr>
<td></td>
<td>/VIRSA/Z_CC.BUSINESS_OWNER</td>
</tr>
<tr>
<td></td>
<td>/VIRSA/Z_CC_USER_ ADMIN</td>
</tr>
<tr>
<td></td>
<td>Version 5 (UME):</td>
</tr>
<tr>
<td></td>
<td>CC.BiznessOwner</td>
</tr>
<tr>
<td>GRC Technical Support</td>
<td>Version 4 (R/3):</td>
</tr>
<tr>
<td></td>
<td>/VIRSA/Z_CC_ADMINISTRATOR</td>
</tr>
<tr>
<td></td>
<td>Version 5 (UME):</td>
</tr>
<tr>
<td></td>
<td>CC.Administration</td>
</tr>
</tbody>
</table>
The /VIRSA/Z_CCA_ ADMINISTRATOR (CC.Administration) is the most sensitive role and should be protected. It provides full access to the GRC system including the ability to maintain configuration settings and segregation of duties rules.

**Optimising the SAP control environment**

<table>
<thead>
<tr>
<th>Optimising SAP controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super user access</td>
</tr>
<tr>
<td>Use of simulations</td>
</tr>
<tr>
<td>Set up of effective segregation of duties rules</td>
</tr>
<tr>
<td>Mitigating controls</td>
</tr>
<tr>
<td>Cross system segregation of duties analysis</td>
</tr>
<tr>
<td>Critical access review</td>
</tr>
<tr>
<td>Reporting</td>
</tr>
<tr>
<td>Define responsibilities</td>
</tr>
</tbody>
</table>

Better practice items to consider in the use of RAR include:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super user access</td>
<td>Super user access should be controlled by the GRC Superuser Privilege Management product, eliminating segregation of duties conflicts relating to users with super user access.</td>
</tr>
<tr>
<td>Use of simulations</td>
<td>Simulations provide the ability to perform preventative segregation of duties testing before allocating user access or modifying SAP security roles. Embedding simulation activities within security processes is critical to ensure ongoing segregation of duties compliance.</td>
</tr>
</tbody>
</table>
| Set up of effective segregation of duties rules | Configuring the segregation of duties ruleset is complex. The default ruleset delivered with enterprise control solutions are incomplete and require localisation.  
The inclusion of additional and custom transactions and modification of authorisation object rules is required. This is rarely performed effectively resulting in the reporting of false positives and wasted remediation effort. |
| Mitigation controls                          | Limit reliance on mitigation controls. Segregation of duties concerns should be fixed through changes in the organisational structure by changing the security structure.                                      |
## Feature article: GRC Access Control

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross system segregation of duties analysis</td>
<td>Version 5 allows the performance of cross system segregation of duties analysis. Cross system analysis allows the evaluation of the adequacy of segregation of critical duties which cross two SAP instances/systems. This is particularly important where the SAP Supplier Relationship Management (SRM) product is used for online purchasing. Where SRM is used, it is important to assess the adequacy of segregation between key SAP functions such as Vendor Maintenance and functions within SRM such as the approval of shopping carts.</td>
</tr>
<tr>
<td>Critical access review</td>
<td>Typically, significant focus is placed on the analysis and correction of segregation of duties issues when implementing Risk Analysis and Remediation. However, it is also important to focus on the adequacy of access to critical and sensitive functions. When using Version 4 of Risk Analysis and Remediation, critical access reviews can be enabled using one of the four matrices provided with the product. Version 5 provides the ability to create critical access and permission rulesets which allow for effective evaluation of the adequacy of access to critical functions.</td>
</tr>
<tr>
<td>Reporting</td>
<td>The effectiveness of inherent reporting within RAR should be considered as part of the RAR implementation project. The adequacy and user friendliness of the reporting of segregation of duties conflicts is critical in ensuring the success and efficiency of the segregation of duties remediation process.</td>
</tr>
<tr>
<td>Define responsibilities</td>
<td>Responsibilities for the use of RAR should be defined and documented. The various responsibilities of Information Technology, business and audit teams must be defined for implementing, monitoring and maintaining the RAR configuration. Organisation-wide commitment is required to effectively implement the tool and remEDIATE segregation of duties concerns. Implementations often become an IT project with limited business involvement.</td>
</tr>
</tbody>
</table>
Superuser Privilege Management

Superuser Privilege Management, also known as Firefighter (FF), provides the ability to address a common audit issue that arises when users have privileged access to the SAP production system. Users log into the FF product instead of using their own access to fix production system issues. FF then logs access which can be subsequently reviewed. The following diagram provides an overview of key capabilities of the FF product:

Overview of SAP Firefighter capabilities

![Diagram of SAP Firefighter capabilities]

Source: Protiviti Australia

SAP security roles are assigned to each FirefightID. Each Firefighter is assigned specific FirefightIDs for a designated period of time (a date range). Once a Firefighter initiates the Firefighter application only FirefightIDs assigned to them are displayed and available for use. Each time a Firefighter logs in using a FirefightID the login event and any subsequent transaction usage is recorded.
### Business roles with which Firefighter is designed for use

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FirefightID Administrator</td>
<td>FirefightID administrators maintain the configuration of the FF system. They also assign FirefightIDs to Firefighters and Controllers.</td>
</tr>
<tr>
<td>Controller</td>
<td>FirefightID Controllers monitor FirefightID usage by reviewing the Log report and receiving email notifications of FirefightID login events. The FF Controller should verify that the transactions executed are appropriate based on the reasons and activities noted by the FF Firefighter. The FF Controller should also maintain evidence of this review.</td>
</tr>
<tr>
<td>Firefighter</td>
<td>Firefighters use the FirefightID logins to run transactions during emergency situations. Firefighters should document the reason and activities performed during the performance of emergency support, including the programs being maintained or transaction codes executed.</td>
</tr>
</tbody>
</table>

The typical process employed when using FF is outlined in the diagram below:

**Example process for use of Firefighter**

1. **Request and/or problem occurs that requires additional access to perform**
2. **User logs into FF via own SAP ID to complete the request and/or resolve the problem**
3. **Controller receives an email alert when the user logs into the Firefighter ID**
4. **Once the task is completed the user logs out of the FF ID. Controller receives an email notification with log report (transaction usage).**
5. **Controller reviews the activities performed by user for appropriateness and maintains evidence of review**
Commonly identified control weaknesses

The following control weaknesses typically occur in FF implementations:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to effectively review FF logs</td>
<td>The entire premise of the FF product is to log and enable review of production system access by users with privileged access. Often, although FF is implemented correctly, Controllers fails to effectively review FF logs.</td>
</tr>
<tr>
<td>Definition of an appropriate set of critical transactions</td>
<td>To enable logging of FF activity it is important to define a set of critical transactions that are considered a risk to the entity. Failure to define an appropriate set of critical transactions results in the inefficient logging of FF activity and often the failure to effectively review FF actions.</td>
</tr>
<tr>
<td>Inappropriate use of FF</td>
<td>Some entities use FF as a solution to segregation of duties concerns or to fix critical access problems. FF should only be used for Firefighting and support purposes.</td>
</tr>
<tr>
<td></td>
<td>For example, a user may have a segregation of duties concern between vendor maintenance and invoice entry. To address this issue, some entities remove one side of the conflict from the user and provide this access through the use of a FF ID. This approach increases the frequency of use of FF, subsequently reducing the effectiveness of the tool.</td>
</tr>
</tbody>
</table>

Significant risks

**High**
- Inadequate Firefighter configuration
- Failure to effectively review Firefighter activity logs

**Medium**
- Using Firefighter to remediate segregation of duties issues rather than for support purposes.
- Definition of an incorrect set of critical transactions
## Risks and controls

### R554: Inadequate Firefighter configuration

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>FF contains a number of overall configuration settings that should be configured correctly to enable effective reporting and monitoring of FF activities.</td>
</tr>
<tr>
<td>Controls</td>
<td>The following table outlines the available configuration options within FF and the recommended settings. Only the configuration options that impact on the control environment are listed (C1016):</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description / Importance of Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieve Change Log</td>
<td>This configuration option determines whether logging is only performed over which transaction codes the user executed or whether change information is also recorded. To capture the transaction and the change log information, set this parameter to <strong>Yes</strong>. To capture only the transaction log information, set this parameter to <strong>No</strong>.</td>
<td><strong>Yes</strong></td>
</tr>
<tr>
<td>Critical Transaction Table from Risk Analysis and Remediation</td>
<td>Use Superuser Privilege Management to maintain and report only critical transactions in logs. The same feature is available from RAR. To use the critical transactions defined in Risk Analysis and Remediation, set this parameter to <strong>Yes</strong>. To use the critical transaction defined in Superuser Privilege Management, set this parameter to <strong>No</strong>.</td>
<td><strong>No</strong>. Critical transactions defined in RAR have a different purpose.</td>
</tr>
<tr>
<td>Assign FF Roles instead of FF IDs</td>
<td>This parameter switches the interface from Firefighter ID-based administration to Firefighter role-based administration. (Default) To use Firefighter IDs, set this parameter to <strong>No</strong>. To use Firefighter roles, set this parameter to <strong>Yes</strong>.</td>
<td><strong>No</strong></td>
</tr>
<tr>
<td>Default Role Expiration in Days</td>
<td>This parameter is in effect only when the Assign Superuser Privilege Management Roles Instead of Firefighter IDs parameter is set to <strong>Yes</strong>. To specify the number of days in which the role expires, set a From date for the Firefighter in the dashboard. The To date increments by the number of days specified for this parameter. If days is not specified, the date today is the From date, and the To date increments by the value set for Default Role Expiration in Days. Dates can manually be selected from the SAP calendar.</td>
<td>Not Applicable. Firefighter IDs should be used.</td>
</tr>
</tbody>
</table>
R554: Inadequate Firefighter configuration (continued)

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description / Importance of Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefighter Owner Additional Authorisation</td>
<td>Each Superuser Privilege Management has a defined owner. This parameter overrides the defined owner privileges. To allow only the defined owner of a Firefighter ID to view and assign the Firefighter ID, set this parameter to Yes. To allow any owner to view and assign that Firefighter ID, set this parameter to No.</td>
<td>Yes</td>
</tr>
<tr>
<td>Configuration Change Comment Mandatory</td>
<td>This parameter adds a mandatory comment to the Configuration Change Log Report. To make this comment mandatory, set this parameter to Yes. To make this comment optional, set this parameter to No.</td>
<td>Yes</td>
</tr>
<tr>
<td>Controller Additional Authorisation</td>
<td>This parameter provides additional authorisation to a Controller. To allow only the user to maintain Controllers for those Firefighter IDs for which the user is owner or administrator, set this parameter to Yes. To allow any user to maintain Controllers, set this parameter to No.</td>
<td>Yes</td>
</tr>
<tr>
<td>Send Log Report Critical Transactions Only</td>
<td>Use this parameter to send log reports with critical transactions to the Controller as an email attachment. To send a log report that contains only critical transactions to Controllers, set this parameter to Yes. To send a log report that contains all transactions to Controllers, set this parameter to No.</td>
<td>Not Applicable. Firefighter IDs should be used.</td>
</tr>
<tr>
<td>Send Log Report Execution Notification</td>
<td>The Send Log Report Execution Notification parameter specifies whether log reports that contain information about Firefighter activity are emailed to Controllers. To send email to a Controller with Firefighter log information, set this parameter to Yes. To send no log information to the Controller, set this parameter to No.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# R554: Inadequate Firefighter configuration (continued)

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description / Importance of Setting</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Send Log Report Execution Notification Immediately</strong></td>
<td>This option specifies whether the log reports should be sent to the Controllers as soon as the background job (/VIRSA/ZVFATBAK) is executed or at a predefined date and time. Note: For the job to run at different intervals an external scheduling tool is required.</td>
<td>Depends on whether scheduling will be used</td>
</tr>
<tr>
<td></td>
<td>To send log report email notifications to the Controller inboxes as soon as the /VIRSA/ZVFATBAK job runs, set this parameter to Yes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To receive the job at regular intervals, schedule the job /VIRSA/ZVFAT_LOG_REPORT at regular intervals, and set this parameter to No.</td>
<td></td>
</tr>
<tr>
<td><strong>Send Firefighter ID Logon Notification</strong></td>
<td>This option specifies whether to send logon notification email to controllers with information about when a Firefighter session was started and by which user.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>To send an email to a Controller with Firefighter logon information, set this parameter to Yes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To send no email with Firefighter logon information to a Controller, set this parameter to No.</td>
<td></td>
</tr>
<tr>
<td><strong>Send Logon Notification Immediately</strong></td>
<td>This option specifies whether the logon notifications should be emailed to the Controllers as soon as they are run or when they are scheduled.</td>
<td>Depends on whether scheduling will be used</td>
</tr>
<tr>
<td></td>
<td>To send an email to a Controller with Firefighter ID logon information after each logon session, set this parameter to Yes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To schedule the /VIRSA/ZVFAT_LOG_NOTIFICATION report at regular intervals, set this parameter to No.</td>
<td></td>
</tr>
</tbody>
</table>
### R555: Failure to effectively review Firefighter activity logs

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>The effectiveness of the FF product in addressing superuser privilege access is contingent of the adequacy of review of FF activity logs by Controllers. Review activities are unable to be adequately performed by Controllers as logs contain deficient data due to poor configuration.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>Appropriate population of critical transaction list</strong></td>
</tr>
<tr>
<td></td>
<td>Ensure that the critical transaction list, which drives activity monitoring, is appropriately populated. This will reduce the amount of activity that is recorded on the FF logs. (C1017)</td>
</tr>
<tr>
<td></td>
<td><strong>Manual controls</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Define roles and processes for review of FF logs (C1018)</strong></td>
</tr>
<tr>
<td></td>
<td>The review of FF logs should be split by functional area. Controllers who understand their area of review are more likely to effectively review FF activity logs. Processes for reviewing FF logs should be documented. These processes should include:</td>
</tr>
<tr>
<td></td>
<td>• Frequency of review.</td>
</tr>
<tr>
<td></td>
<td>• Action to be undertaken if unusual activities are identified.</td>
</tr>
<tr>
<td></td>
<td>• The evidence required to be maintained.</td>
</tr>
</tbody>
</table>
R556: Using Firefighter to remediate segregation of duties issues rather than for support purposes.

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>The FF product is used to address critical access or segregation of duties issues rather than for performing periodic or on demand production support. For example, a user may have access to create vendor and process invoices which breaches a segregation of duties rule. Instead of removing either vendor maintenance or invoice entry, the user is given invoice entry ability through a FF ID. This is an ineffective use for FF as it is not designed to address segregation of duties risks.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><strong>FF should only be used for performing production system support</strong></td>
</tr>
<tr>
<td></td>
<td>The product should not be used to address segregation of duties risks or for other development activities. The following outlines typically acceptable and unacceptable uses for FF: (C1019)</td>
</tr>
<tr>
<td></td>
<td>• Usage practices that support the effective use of FF.</td>
</tr>
<tr>
<td></td>
<td>• Opening and closing posting periods.</td>
</tr>
<tr>
<td></td>
<td>• Backup activities.</td>
</tr>
<tr>
<td></td>
<td>• Basis activities.</td>
</tr>
<tr>
<td></td>
<td>Ineffective practices include:</td>
</tr>
<tr>
<td></td>
<td>• FF should not be used to address segregation of duties or critical access issues. For example, FF may be used to review one side of a segregation of duties conflict.</td>
</tr>
<tr>
<td></td>
<td>• FF should not be used for long periods of time.</td>
</tr>
<tr>
<td></td>
<td>• FF should not be used on a frequent basis.</td>
</tr>
<tr>
<td></td>
<td>• FF should not be used for development in production as development activities should occur in the appropriate development system and follow the SAP Change Control Policy to migrate the change to Production.</td>
</tr>
</tbody>
</table>
R557: Definition of an incorrect set of critical transactions

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Incorrect definition of the critical transaction listing can result in ineffective monitoring of FF activity. Only transactions that present a critical or moderate risk should be included. Inclusion of transactions that present no or a low risk increase the size of the FF activity logs and reduce the effectiveness of the Controller’s review of FF logs.</td>
</tr>
</tbody>
</table>

Controls

**Manual controls**

*Identification of critical transactions*

During the implementation of FF, a risk assessment should be performed to identify critical transactions that present a critical or moderate risk. Critical transactions typically include master data processes like vendor or customer maintenance, or key financial transaction postings like invoice entry. (C1020)

Security considerations

The following table outlines standard security roles that are delivered within FF:

<table>
<thead>
<tr>
<th>Role</th>
<th>GRC RAR Security Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>/VIRSAZ_VFAT_ADMINISTRATOR</td>
</tr>
<tr>
<td>Owner / Controller</td>
<td>/VIRSAZ_VFAT_ID_OWNER</td>
</tr>
<tr>
<td>Firefighter</td>
<td>/VIRSAZ_VFAT_FIREFIGHTER</td>
</tr>
</tbody>
</table>

In addition:

- Access to the Administrator role should be restricted to key FF Administrators given it provides the ability to maintain configuration parameters.
- Firefighters should not be provided with the access to either the Administrator or Owner / Controller roles.
Optimising the SAP control environment

Better practice items to consider in the use of FF include:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish descriptive reason codes</td>
<td>Reason codes describe each task that a Firefighter expects to perform. For example, a reason code might be a technical support case number. The reason code should be clear, so that the Firefighter understands the task that it represents. To enable users to search or filter the Reason and Activity report, or the Log Report by reason code, the reason code must be a lookup.</td>
</tr>
<tr>
<td>Focus on the effectiveness of review of FF Logs</td>
<td>The adequacy of Controller review of FF logs should be periodically assessed. This process should involve periodic assessments of the evidence maintained by each Controller for the review of activity logs.</td>
</tr>
</tbody>
</table>
Chapter 6

Controlling

Overview 199
Functional overview 200
Commonly identified control weaknesses 201
Significant risks 201
Risks and controls 202
Security considerations 205
Optimising the SAP control environment 207
IMPORTANT UPDATE
Overview

The Controlling (CO) module is primarily used for management reporting purposes. Its central function is to report exclusively on revenues and costs. In addition to analysing actual data, one of the key elements of Controlling is recording and monitoring of planned and budget data.

The difference between a Cost Centre and a Profit Centre is that the Cost Centre represents individual costs incurred during a given period and Profit Centres contain the balances of both costs and revenues.

Controlling (CO) and Financial Accounting (FI) are independent, yet closely integrated. All data relevant to costs and revenues are transferred automatically in near real time to CO from FI. This data is assigned by the system to different CO accounts, such as cost centres, business processes, projects, or orders. The relevant accounts in FI are managed in CO as either cost or revenue elements, which enables comparison and reconciliation of the values from the two modules.

While the CO module does not present significant risk to the accuracy or completeness of the financial statements but is important if reliance is placed on Cost Centre manager review of expenditure and revenue items.
Functional overview

The CO module consists of the following components:

- **Cost Element Accounting (CO-OM-CEL)**: Allows the viewing of overview of the costs and revenues that occur in an entity with actual data directly from Financial Accounting. These cost elements are the basis for cost accounting, enabling the user to display costs for each of the accounts that have been assigned to the cost element.

- **Cost Centre Accounting (CO-OM-CCA)**: Allows the display of costs incurred by the business, as allocated to Cost Centres. Cost Centres can be created for such functional areas as Marketing, Purchasing, Human Resources, Finance, Legal, etc. Cost Centre Accounting can be used for planning, budgeting and reporting. It also gives management visibility of functional departments/areas of the entity and the ability to distribute costs to other cost objects.

- **Activity-Based Accounting (CO-OM-ABC)**: Allows additional capabilities for allocating costs to products based on the cross-departmental processes performed by the entity. Activity-based accounting seeks to optimise business flows with the goals of the entire entity in mind.

- **Internal Order Accounting (CO-OM-OPA)**: Allows tracking of costs as incurred by a specific job, service, project, or task. Internal Orders are a method of collecting these costs related to that task. Budgets can be assigned to assist in ensuring these order costs are not exceeded.

- **Product Cost Controlling (CO-PC)**: Allows for the calculation the costs of the product being manufactured or the service provisioned. This allows management to make a decision on the optimal price to market their product.

- **Profitability Analysis (CO-PA)**: Allows the calculation of operating profit and contribution margins by individual market segments. This analysis provides management with information for decision making through two methods:
  - Account-Based Analysis – cost and revenue element accounts are used to provide valuation
  - Cost-Based Analysis – gains valuation using a user-defined costing approach

- **Profit Centre Accounting (EC-PCA)**: Allows the evaluation of profit and loss for individual profit centres, as well as return on investment (ROI), working capital, and cash flow. Profit Centres can be set-up to identify product lines, divisions, geographical regions, offices, production sites, or by functions. This makes it possible to evaluate different areas of responsibility within the entity.
Commonly identified control weaknesses

The following control weaknesses typically occur in the Controlling module:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controlling master data set up</td>
<td>The accuracy and integrity of the Cost Centre and Profit Centre reporting is dependent on the effective maintenance of Controlling master data items. There are typically integrity concerns with Controlling master data, including duplicate cost elements and the allocation of incorrect segment items to Cost and Profit Centres.</td>
</tr>
<tr>
<td>Financial and Controlling</td>
<td>The integration of the Financial Accounting and Controlling modules is vital to the integrity of management reporting from Controlling. Entities often fail to effectively reconcile the FI and CO modules correctly.</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>Review of Cost Centre reports by Managers is a critical control to ensure the accuracy and appropriateness of cost allocations. It is important that cost centre managers regularly review cost centre reports and follow up on possible exceptions.</td>
</tr>
<tr>
<td>Cost Centre Manager Review</td>
<td>Issues are often identified with the timely settlement of costs items allocated to Internal Orders.</td>
</tr>
</tbody>
</table>

Significant risks

- Reconciliation problems between the FI and CO modules
- Ineffective maintenance of CO master data
- Incorrect allocations or reversal of costs to Cost Centres
- Incorrect or failure to settle internal order costs

- Cost Structure Maintenance and Cost Centre Transfer
- Cost Structure Maintenance and AP Invoice Entry
- Cost Structure Maintenance and Purchase Orders
- Internal Order Maintenance and Settle Internal Order Costs
Risks and controls

R600: Reconciliation problems between the FI and CO modules

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Before ECC, the FI and CO modules were not fully integrated in real time. This created the requirement to regularly reconcile revenue and cost items between the General Ledger and the CO module. To ensure the integrity of costing and management reporting, it is critical to regularly reconcile the Financial Accounting and Controlling modules. <em>Implementation of the New General Ledger reduces the risk of reconciliation problems between the CO and FI modules.</em></td>
</tr>
</tbody>
</table>

Controls

- **Configuration controls**
  - Activating elements that interface into the financial modules
    - The modules that interface into the financials modules are defined within table TRWCA. It is possible to activate elements that interface into the financial modules as well as define a fiscal year for which the element is active. (C744)

- **Manual controls**
  - Running Controlling to Financials Reconciliation report
    - The Controlling to Financials Reconciliation report enables the comparison of costs posted on individual cost elements to expenses recorded in financial accounting. It should be run on a regular basis to identify reconciliation problems. (C715)

- **Reconciliation ledger**
  - The reconciliation ledger is a useful control to ensure reconciliation between internal and external accounting. All sender and receiver information from affected documents is stored in the ledger. (C745)
R601: Ineffective maintenance of CO master data

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Failure to maintain accurate controlling master data, including primary and secondary cost elements, can impact on the integrity and accuracy of management reporting.</td>
</tr>
</tbody>
</table>

**Controls**

**Configuration controls**

*Allocation of planned and actual costs*
To enable effective allocation of planned and actual costs it is important to establish effective Controlling area configuration. It is important that the currency type, assignment control, currency, chart of accounts, and fiscal year variant are established correctly. (C950)

**Mandatory fields**
Mandatory fields (screen variants) can be configured for the following Manual Actual Postings, using the identified transaction code: – cost element number – name – type – Cost Centre number. (C735)

**Cost Centre accounting and validation**
For each Controlling area it is possible to define whether Cost Centre accounting is active. These configuration options also define whether validation against Controlling master data is performed. (C738)

**Manual controls**

*Review for duplicate Cost Centres*
When new Cost Centres are created, a review for duplicate Cost Centres should be performed. (C732)

*Reports to monitor changes to CO master data*
There are the following three reports that can be used to monitor changes to Controlling master data: (C718)
- Cost elements: master data reports
- Cost Centres: master data reports
- Internal Orders: master data reports
### R602: Incorrect allocations or reversal of costs to Cost Centres

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Costs from the Financial Accounting module may be incorrectly allocated to or reversed from a Cost Centre. This can impact on the integrity and accuracy of management reporting.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
<tr>
<td>Review of financial and CO reports</td>
<td>Cost Centre managers should review financial and Controlling reports to identify costing allocation and settlement problems as well as incorrect splitting of costs between activity types. (C748)</td>
</tr>
</tbody>
</table>

### R603: Incorrect or failure to settle internal order costs

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Internal order settlement rules may be incorrectly established, potentially resulting in the incorrect settlement of expenditure to assets or the failure to settle asset items. This can impact on the integrity of the expenditure and asset items recording in the financial statements.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td>Use of settlement profiles</td>
<td>Each internal order type should be assigned to a settlement profile. (C749)</td>
</tr>
<tr>
<td>Configuration of system messages for Controlling</td>
<td>System messages for Controlling should be set. Generally, the key system messages should apply to all users and not a specific user. To improve the control environment, key Controlling system messages, such as where the settlement profile does not allow the settlement of costs, should be set to an error. (C707)</td>
</tr>
<tr>
<td>Manual controls</td>
<td>Accounting policies and procedures</td>
</tr>
<tr>
<td>Periodic review of internal order settlement rules</td>
<td>Transaction KOSRLIST_OR. The internal order settlement rule report is useful to review the adequacy of allocated settlement rules. The accuracy of settlement rules is critical to ensure correct allocation of costs and the settlement of assets. (C723)</td>
</tr>
<tr>
<td>Periodic review of internal orders</td>
<td>Transaction S_ALR_87013010 Internal Order breakdown report can be used to identify internal orders that have not been appropriately closed. (C724)</td>
</tr>
</tbody>
</table>
Security considerations

Standard Controlling security objects that should be restricted to appropriate staff

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td>Description</td>
</tr>
<tr>
<td>1KE8</td>
<td>Profit Centre Posting</td>
</tr>
<tr>
<td>KA01, KA02, KA02CORE</td>
<td>Create, Change, &amp; Maintain Cost Elements</td>
</tr>
<tr>
<td>KB15N</td>
<td>Enter Manual Allocations</td>
</tr>
<tr>
<td>KE51, KE52</td>
<td>Create, Change Profit Centre</td>
</tr>
<tr>
<td>KO01, KO02</td>
<td>Create, Change Internal Order</td>
</tr>
<tr>
<td>K088</td>
<td>Actual Settlement: Order</td>
</tr>
<tr>
<td>KS01, KS02</td>
<td>Create, Change Cost Centre</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td>Protects manual cost postings and allocation of planned and actual costs.</td>
</tr>
<tr>
<td>V_KRGNG</td>
<td>Protects the maintenance of Cost Centre master data.</td>
</tr>
<tr>
<td>K_CSKS</td>
<td>Protects the maintenance of Cost Centre master data.</td>
</tr>
<tr>
<td>Entity Values</td>
<td></td>
</tr>
<tr>
<td>BUKRS</td>
<td>Company Code</td>
</tr>
<tr>
<td>GSBER</td>
<td>Business Area</td>
</tr>
<tr>
<td>KOKRS</td>
<td>Controlling Area</td>
</tr>
<tr>
<td>PRCTR</td>
<td>Profit Centre</td>
</tr>
</tbody>
</table>
### Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost Structure Maintenance</td>
<td>Cost Centre Transfer</td>
<td>Create an incorrect Cost Centre or manipulate existing Cost Centre details and use Cost Centre transfer to move fraudulent costs between cost centres. This risk is particularly critical when script cost centre budgeting and review is considered a key management control.</td>
</tr>
<tr>
<td>Cost Structure Maintenance</td>
<td>AP Invoice Entry</td>
<td>User may enter false vendor invoice and post this to an invalid Cost Centre to avoid detection.</td>
</tr>
<tr>
<td>Cost Structure Maintenance</td>
<td>Purchase Orders</td>
<td>User may reallocate a purchase order to an inappropriate Cost Centre (Balance Sheet or Income Statement), resulting in inaccurate financial reporting.</td>
</tr>
<tr>
<td>Internal Order Maintenance</td>
<td>Settle Internal Order Costs</td>
<td>A user with the ability to create a fictitious internal order or manipulate an existing internal order and settle that order can hide inappropriate costs or fraudulent payments.</td>
</tr>
</tbody>
</table>
### Optimising the SAP control environment

**Optimising SAP controls**
- FI/CO Reconciliation
- Pre-deletion analysis of dependent of Controlling Master data

Better practice procedures to improve Controlling module controls include:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
</table>
| FI/CO Reconciliation | Appropriate General Ledger adjustment accounts should be created to allow for reconciliation postings from the FI/CO reconciliation ledger. These accounts should be defined as ‘profit and loss accounts’ and should not be used for other transactions in the FI module. Accounts should be appropriately configured according to the object classes and transactions used.  

The FI/CO reconciliation should be performed as a test run prior to the actual reconciliation. The results of the test run should be reviewed by management prior to processing the reconciliation posting.  

The implementation of the New General Ledger reduces reconciliation problems between the CO and FI modules.  

*Chapter 3: General Ledger – Section 3.3 New General Ledger* |
| Deletion of Controlling master data | A test run function is available to check whether master data selected for deletion has any dependencies that may cause issues, should the deletion process take place. The test run completes extensive checks of dependent data; reporting on data that might be affected by the proposed deletion(s), and preventing deletion where dependent data is present. |
Chapter 7

Project System

Functional overview 211
Commonly identified control weaknesses 212
Significant risks 212
Risks and controls 213
Security considerations 217
Optimising the SAP control environment 218
IMPORTANT UPDATE
Functional overview

Projects are a part of the internal workings of most entities. They may vary considerably in size from the large scale of building a new warehouse or implementing a new ERP software system like SAP, to the smaller scale of a compliance audit. However, all projects have commonalities that include a list of tasks that must be completed, a budget, and a specific time for completion. A clear, unambiguous project structure is the basis for successful project planning, monitoring, and control.

The SAP Project System (PS) module facilitates project management activities, including project planning through to completion of the project and provides for project monitoring. The PS component is highly integrated with the other SAP application components, which improves user access to real-time project relevant cost data from across the entity. This allows an entity to plan, execute, and account for projects as part of normal commercial procedures.

One of the key requirements of the PS is to map the structure of each project. Key elements of the project structure are:

- **Work Breakdown Structure**: The project is first broken down into work breakdown structures (WBS) which map to specific project deliverables.
- **Network of Project activities**: Each WBS element can then be broken down into networks of activities. A network can be thought of as a list of tasks organised into a process flow with specific timing.
- **Project activities**: Activities are the key tasks to be completed. These activities map to internal activities, external activities, cost activities, and materials components.
- **Work centres**: Internal activities are assigned to work centres (resources) to be completed.
Commonly identified control weaknesses

Common control weaknesses that typically occur in the Project System module:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity concerns with WBS / Project</td>
<td>Integrity concerns with project and WBS element set up can impact on the effective management and reporting / settlement of project costs.</td>
</tr>
<tr>
<td>structures</td>
<td></td>
</tr>
<tr>
<td>Incorrect establishment of settlement</td>
<td>Settlement rules are complex and difficult to establish. Often incorrect settlement rule configuration results in problems with the settlement of project costs into either the General Ledger or Asset module.</td>
</tr>
<tr>
<td>rules</td>
<td></td>
</tr>
<tr>
<td>Untimely settlement of costs</td>
<td>Project costs are not always settled on a timely basis to ensure the integrity of cost and asset amounts.</td>
</tr>
</tbody>
</table>

Significant risks

**High**
- Incorrect set up or changes to project or WBS structures
- Configuration issues with settlement rules
- Inadequate project justification or unapproved projects
- Inadequate management of project timeframes, deliverables and costs

**Medium**
- Projects are not closed or are closed with open commitments
- Project System does not interface to the General Ledger

**Segregation of duties risks**
- Define WBS Elements and Project Settlement
- Define WBS Elements and Overhead Posting
- Project Settlement and Asset Master Record Maintenance
- Project Settlement and Overhead Posting Functions
## Risks and controls

<table>
<thead>
<tr>
<th>R700: Incorrect set up or changes to project or WBS structures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk rating</strong></td>
</tr>
<tr>
<td><strong>Risk description</strong></td>
</tr>
<tr>
<td><strong>Controls</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
R701: Configuration issues with settlement rules

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Incorrect settlement rules can result in expenditure items being incorrectly capitalised as an asset record or conversely an asset record being incorrectly expensed. This will impact on the accuracy of asset and expenditure records, increasing the risk of financial misstatement.</td>
</tr>
</tbody>
</table>
| Controls | Configuration controls  
Settlement profile configuration  
Settlement profiles are created for various items such as overhead costs or particular types of orders. For each settlement profile it is possible to define whether costs are to be settled. It is important that settlement profiles for key order types settle all allocated costs. (C773)  
Settlement profiles are created for various items such as overhead costs or particular types of orders. For each settlement profile it is possible to define the valid cost receiver as a result of cost settlement. It is important that all profiles that facilitate capitalisation have assets as a receiver. (C775)  
Manual controls  
Inclusion of a review of the creation of each project  
Project approval procedures should include a review of the creation of each project, including the allocated order type. |

R702: Inadequate project justification or unapproved projects

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Ineffective documentation and cost benefit justifications for projects could lead to undesirable projects set up in the system. In addition, projects may not be approved in accordance with entity delegations.</td>
</tr>
</tbody>
</table>
| Controls | Manual controls  
Project approval policies and procedures  
Most entities implement a policy stating requirements for project documentation, such as key information to be included in business cases. Projects should be fully documented, including relevant risks and costs/benefits. Projects should be approved in accordance with the entity’s delegation of authorities. (C779) |
<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
</table>
| Risk description | Ineffective project management processes can result in a number of inefficiencies including the failure to:  
- Establish an appropriate and realistic budget;  
- Monitor project actual to budget resulting in project cost overruns;  
- Obtain materials on a timely basis to meet project requirements;  
- Monitor the achievement of key deliverables and timeframes; or  
- Manage scope changes effectively. |
| Controls | Configuration controls  
Management of budget profiles  
It is important to establish and allocate a budget profile to each project. Realistic budgets should be set and assigned against each project phase. (C767)  
Availability functionality can be used to control budget overruns. A budget dollar and percentage overrun tolerance can be establish. (C768)  
Manual controls  
Monitoring project process  
Project System functionality is used to monitor project progress against budget and key milestones. (C771)  
Approval of changes to project scope  
All project scope changes should be reviewed and appropriately approved. (C781) |
R704: Projects are not closed or are closed with open commitments

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>The accuracy and completeness of financial reporting of project or capital costs may be impacted. Failure to close old projects can result in unauthorised or fraudulent expenditure being hidden in old project codes. This could result in financial loss for the entity.</td>
</tr>
</tbody>
</table>
| Controls | Configuration controls

**Automatic date notification process**
The Project System contains automatic date notification functionality which can be used to notify management on the occurrence of key Project System events. An automatic date notification can be set up to notify management of key events, such as the need to raise an invoice for project services. (C770)

**Manual controls**

**Monitoring and review of current projects**
Regular review of open projects should be performed to identify projects that have been completed and need to be finalised in SAP. This will ensure that the financial aspects of the project are settled in a timely matter. (C780)

Project managers should address all open items before closing projects. (C873)

R705: Project System does not interface to the General Ledger

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Failure to correctly interface the General Ledger and Projects System will result in reconciliation problems and the failure to accurately reflect project costs within the financial statements.</td>
</tr>
</tbody>
</table>
| Controls | Configuration controls

**Setting Project System interface to the General Ledger**
The Project System interface to the General Ledger must be set as Active within table TRWCA. The year that the interface will operate until must also be defined. (C789)

Chapter 3: General Ledger
Security considerations

Standard Project System security objects that should be restricted to appropriate staff

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td></td>
</tr>
<tr>
<td>CJ01, CJ02</td>
<td>Create, Change Work Breakdown Structure</td>
</tr>
<tr>
<td>CJ11, CJ12</td>
<td>Create, Change WBS Element</td>
</tr>
<tr>
<td>CJ44, CJ45</td>
<td>Act. overhd: Projects; Ind. process., Coll. process.</td>
</tr>
<tr>
<td>CJ46, CJ47</td>
<td>Pind ovhd: Projects, Ind. process., Coll. process.</td>
</tr>
<tr>
<td>CJ88</td>
<td>Settle Projects and Networks</td>
</tr>
<tr>
<td>CJ8G</td>
<td>Actual Settlement: Projects/Networks</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>C_PROJ_TCD</td>
<td>PS: Transaction-Specific Authorisations in Project System</td>
</tr>
<tr>
<td>C_PRPS_ART</td>
<td>PS: Project type authorisation for WBS elements</td>
</tr>
<tr>
<td>C_PRPS_KOK</td>
<td>PS: Controlling Area Authorisation for WBS elements</td>
</tr>
<tr>
<td>C_PRPS_KST</td>
<td>PS: Cost Centre Authorisation for WBS elements</td>
</tr>
<tr>
<td>C_PRPS_PRC</td>
<td>PS: Profit Centre Authorisation for WBS elements</td>
</tr>
<tr>
<td>C_PRPS_VNR</td>
<td>PS: Project Manager Authorisation for WBS elements</td>
</tr>
<tr>
<td>Entity Values</td>
<td></td>
</tr>
<tr>
<td>KOKRS</td>
<td>Controlling area</td>
</tr>
<tr>
<td>PRCTR</td>
<td>Profit centres</td>
</tr>
</tbody>
</table>
Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define WBS Elements</td>
<td>Project Settlement</td>
<td>Ability to maintain WBS elements and perform project settlement can result in the incorrect settlement of costs, potentially to hide fraudulent activity.</td>
</tr>
<tr>
<td>Define WBS Elements</td>
<td>Overhead Posting</td>
<td>Maintenance of the work breakdown structure and manipulation of overhead postings can result in incorrect financial and management reporting.</td>
</tr>
<tr>
<td>Project Settlement</td>
<td>Asset Master Record Maintenance</td>
<td>A user could create a fictitious asset without going through the settlement approval process.</td>
</tr>
<tr>
<td>Project Settlement</td>
<td>Overhead Posting</td>
<td>A user could post incorrect overhead postings to a project and then settle that project to hide the costs.</td>
</tr>
</tbody>
</table>

Optimising the SAP control environment

- Scope Changes
- Period Comparison Report
- Project Information System
- Project Monitoring
- Project and WBS Element Approval
- Availability Checking
Better practice items that can assist in improving Project System controls include:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope Changes</td>
<td>One of the key success factors in the management of any project is the effective management of project scope. All scope changes must be documented, justified and appropriately approved by management.</td>
</tr>
<tr>
<td>Period Comparison Report</td>
<td>Project System includes a Period Comparison Report which can be used to compare costs charged to a project across the periods. The report should be reviewed to identify unusual project cost allocations.</td>
</tr>
<tr>
<td>Project Information System</td>
<td>The project information system can be used for a variety of purposes including reviewing revenue and cost items allocated to individual projects. The project information system can also be used to identify potential duplicate projects.</td>
</tr>
<tr>
<td>Project Monitoring</td>
<td>Project progress is updated into the Project System via numerous channels including confirmations, start and finish dates allocated on WBS elements or time sheets for employees. It is important that the project managers regularly assess the progress of projects.</td>
</tr>
<tr>
<td>Project and WBS Element Approval</td>
<td>User status items can be used to implement approval controls over projects and WBS elements. Authorisation user status items are allocated to user accounts.</td>
</tr>
<tr>
<td>Availability Checking</td>
<td>Availability checking can be configured to check the availability of materials for project requirements.</td>
</tr>
</tbody>
</table>

**IMPORTANT UPDATE**
Chapter 7 – Feature article

Grants management

Overview 223
Significant risks 224
Risks and controls 224
Security considerations 225
IMPORTANT UPDATE
Overview

SAP Grants Management is part of the SAP Public Service industry solution. It is typically implemented with the SAP Funds Management component.

Grants Management supports all business processes a grantee must engage in, starting with preparatory activities prior to receiving funds to the accounting and reporting activities required after grants are awarded. With Grants Management, grantees have support for the following activities:

- Prepare grant applications – Support all preliminary activities using centralised document management and built-in workflows.
- Record sponsor’s details – Record the attributes unique to sponsored program management, such as budgeting, cost sharing and matching, billing, and indirect cost and overhead calculations.
- Execute the awarded grant – Manage sponsor receivables, standardise business processes across all organisational units, and automate the budget process. An entity’s financial administrators can manage and control grant transactions and postings and perform availability checks to ensure that expenditures comply with entity budgets.

Although SAP does provide a Grants Management component, entities do not always use this component; instead they use other components of SAP to manage the Grants Management process.

Components of SAP that can be used to manage the Grants Management process

<table>
<thead>
<tr>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project System</td>
<td>Grant projects can be established an individual projects within the Project System. Budgets can be allocated against each project and all project costs can be recorded.</td>
</tr>
<tr>
<td>Controlling / Internal Orders</td>
<td>Grant projects can be set as internal orders within the Controlling module.</td>
</tr>
<tr>
<td>General Ledger</td>
<td>Grant projects can be established as separate General Ledger accounts. A budget can be established against the account.</td>
</tr>
</tbody>
</table>
Significant risks

High

- Inappropriate establishment approval of each grant project
- Untimely settlement of costs
- Allocation of costs against the incorrect project

Segregation of duties risks

- Approve Grant and Record Grant functions
- Maintain Grant Costs and Settle Project Costs functions

Risks and controls

No matter which element of SAP is used to manage grants, key risks and required controls remain.

R710: Inappropriate establishment approval of each grant project

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Grant projects, whether managed through Grants Management, the Project System, Controlling or the General Ledger, must be appropriately approved before being initiated or else an unauthorised, unapproved grant project may be initiated.</td>
</tr>
<tr>
<td>Controls</td>
<td>Projects should be approved in accordance with the entity’s delegations of authority. Only approved projects should be created within SAP. (C1003) A budget should be established for each grant project. SAP budget availability functionality and reporting can be used to report actual to budget costs. (C1004)</td>
</tr>
</tbody>
</table>

R711: Untimely settlement of costs

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Depending on the way grant projects are set up within SAP, particularly if the Project System is used, it is important that costs recorded against grant projects are settled to the General Ledger on a timely basis. If this is not done, then the General Ledger may be incomplete and not up to date.</td>
</tr>
<tr>
<td>Controls</td>
<td>Procedures for the settlement of project costs should be established and followed when managing project costs. (C1001)</td>
</tr>
</tbody>
</table>
Risk rating: HIGH

Risk description: The process of recording costs against projects must be transparent. A common issue to address is to develop controls and procedures that prevent or detect the recording of costs against an incorrect project.

Controls: Key controls that should be implemented to assess whether costs are recorded against the correct project (C1002). Such controls may include:

- Data entry procedures should ensure that the costs are entered against the correct project.
- All project costs should be appropriately approved. The project approval documentation should contain the relevant grant project that the cost related to.
- Develop reports that enable managers to review actual costs against each Grant project.

Security considerations

Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approve Grant</td>
<td>Record Grant</td>
<td>The ability to approve and record a grant project can result in the creation of unauthorised grant projects.</td>
</tr>
<tr>
<td>Maintain Grant Cost</td>
<td>Settle Project Costs</td>
<td>Ability to maintain WBS elements and perform project settlement can result in the incorrect settlement of costs, potentially to hide fraudulent activity.</td>
</tr>
</tbody>
</table>
Chapter 8

Asset Accounting

8.1 Asset Master Maintenance 230
8.2 Asset Transaction Postings 235
IMPORTANT UPDATE
Overview

The Asset Accounting component of SAP is used for managing and supervising fixed assets. It serves as a subsidiary ledger to the General Ledger, providing detailed information on transactions involving fixed assets.

Traditional asset accounting encompasses the entire lifetime of the asset from purchase order or the initial acquisition (possibly managed as an asset under construction) through to its retirement. The system calculates, to a large extent automatically, the values for depreciation, interest, insurance and other purposes between these two points in time, and places this information in varied form using the Information System. There is a report for depreciation forecasting and simulation of the development of asset values.

The system also offers special functions for leased assets and assets under construction. The system allows for the ability to manage values in parallel currencies using different types of valuation. These features simplify the process of preparing for the consolidation of multi-national group concerns.

From a financial statement perspective, adequate control within the Asset Accounting module is required to ensure accurate recording of depreciation charges. To enable accurate depreciation charges it is important to define a correct chart of depreciation. Values for assets for different needs are required to be calculated, both internal and external (such as book depreciation and cost depreciation). Asset Accounting allows the management of values for assets in parallel in up to 99 depreciation areas.

Asset Accounting is integrated with a number of other SAP components including:

- Posting of asset acquisitions and retirements that are integrated with Accounts Payable and Accounts Receivable.
- Account assignment of down payments to assets when down payments in the Financial Accounting (FI) component are posted.
- Posting of depreciation from Asset Accounting to the appropriate General Ledger accounts.
- Posting of asset records through purchase orders in Materials Management.

The following diagram illustrates the critical functions for SAP Asset Accounting:
8.1 Asset Master Maintenance

Functional overview

The Asset Master within Asset Accounting is used for recording the Master Data of your assets on an individual asset basis. The following outlines the different elements of the Asset Master Record:

General asset master data

This part of the master record contains concrete information about the fixed asset. Key elements of the master record include:

- General information (description, quantity, etc.)
- Account assignment
- Posting information (for example, capitalisation date)
- Time-dependent assignments (for example, cost centre)
- Information for plant maintenance
- Entries for net worth tax
- Information on real estate
- Leasing conditions
- Information on the origins of the asset
- Physical inventory data
- Insurance data

Data for calculating asset values

Depreciation terms may be specified in the Asset Master Record for each depreciation area in the chart of depreciation. In order to make these specifications, the master record contains an overview of the depreciation areas.
Commonly identified control weaknesses

The following control weaknesses typically occur in maintaining Asset Master Records:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory fields for Asset Master Records</td>
<td>Problems with the integrity of asset records often occurs because key fields such as serial number, asset location or cost centre are not set as mandatory.</td>
</tr>
</tbody>
</table>

Significant risks

- **High**
  - High value assets are entered into a low value asset class

- **Medium**
  - Duplicate or incomplete Asset Master Records are created.
  - Asset records on the Asset Register do not exist

Segregation of duties risks

- Asset Master Record Maintenance and Asset Transactions
- Accounts payable Invoices and Asset Master Record Maintenance
- Purchase Order Processing and Asset Master Record Maintenance

Risks and controls

**R800: High value assets are entered into a low value asset class**

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>SAP Assets allows the creation of low value asset classes to increase the efficiency of recording of low value assets. There is a risk that high value assets are recorded in this asset class, resulting in incorrect depreciation charges.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Controls</th>
<th>Configuration controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration of low value asset class</td>
<td>A low value asset class should be created for each company code. To activate the low value asset class a maximum amount should be set per company code or depreciation area. SAP checks the maximum amount during every acquisition posting. (C344) (C548)</td>
</tr>
<tr>
<td>To enable this check, the corresponding <strong>low value indicator</strong> has to be set within the asset class. This control reviews whether the asset class has been set to check for the maximum low value amount. (C547)</td>
<td></td>
</tr>
</tbody>
</table>
## R801: Duplicate or incomplete Asset Master Records are created

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Incomplete or duplicate asset records may be created resulting in incorrect depreciation charges or an inability to locate asset records.</td>
</tr>
<tr>
<td>Controls</td>
<td></td>
</tr>
<tr>
<td><strong>Configuration controls</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Field status</strong></td>
<td>The ‘field status’ for Asset Master Records should be configured to ensure that all fields necessary to complete the record are set to ‘required entry’. Fields which are not always required should be set to ‘optional entry’. Fields which are never required should be set to ‘display only’ or ‘suppressed’. Some fields are set as ‘required entry’ by SAP and cannot be changed (i.e. asset class, company code, description). Additional fields which should be set as ‘required entry’ include business area (if used), cost centre, plant and location. (C345) (C887)</td>
</tr>
<tr>
<td><strong>Manual controls</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Review Asset Acquisition Report</strong></td>
<td>The Asset Acquisition Report (RAZUGA01), Transaction Code AR05, identifies all new asset acquisitions entered into SAP for a selected period. The acquisition report can be reviewed by asset staff to identify incorrect or duplicate asset acquisition postings. (C352)</td>
</tr>
<tr>
<td><strong>Review Changes to Asset Master Records Report</strong></td>
<td>The Changes to Asset Master Records Report using transaction code AR15 should also be periodically reviewed to ensure that all changes made to Asset Master Records were authorised and accurately processed in the system. (C353)</td>
</tr>
</tbody>
</table>
R802: Asset records on the Asset Register do not exist

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Fictitious asset records are recorded within the Asset Register, incorrectly increasing the asset value recorded within the financial statements.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
<tr>
<td></td>
<td><em>Asset class inclusion in Asset Inventory Stock Take Report</em></td>
</tr>
<tr>
<td></td>
<td>It is possible to configure whether an asset class will be included within the Asset Inventory Stock Take Report. If this indicator is not selected, assets within the asset class will not be reviewed in the stock take. (C508)</td>
</tr>
<tr>
<td></td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td><em>Stock takes</em></td>
</tr>
<tr>
<td></td>
<td>Regular stock takes should be performed and results analysed. Stock takes will typically identify whether the recording of acquisitions, disposals and movements is working correctly. (C370)</td>
</tr>
</tbody>
</table>

Security considerations

Transactions of which access should be restricted to relevant Finance/Asset Accounting staff

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td></td>
</tr>
<tr>
<td>AS01</td>
<td>Create Asset Master Record</td>
</tr>
<tr>
<td>AS02</td>
<td>Change Asset Master Record</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>A_S_ANLKL</td>
<td>Asset Maintenance by Company</td>
</tr>
</tbody>
</table>
Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Master Record</td>
<td>Asset Transactions</td>
<td>A user with the ability to maintain Asset Master Records and process asset transactions which including acquisitions, retirements and depreciation actions, could perform a number of inappropriate actions including writing off and misappropriating assets, retiring assets without revenue, and performing inappropriate depreciation activities which can impact the financial statements.</td>
</tr>
<tr>
<td>Maintenance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts Payable Invoices</td>
<td>Asset Master Record</td>
<td>One of the key risks from a financial statement perspective is the ability to hide expenditure as a capitalised asset. A user with the ability to maintain assets and process invoices could create a fictitious asset to hide expenditure as a capitalised asset.</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td></td>
</tr>
<tr>
<td>Purchase Order Processing</td>
<td>Asset Master Record</td>
<td>A user could order a purchase item, pocket the item and write the asset off.</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td></td>
</tr>
</tbody>
</table>

Optimising the SAP control environment

- Align asset classes to entity assets
- Segregate the ability to maintain asset records and purchase orders

Better practice items to consider in the use of Asset Accounting include:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Align asset classes to entity assets</td>
<td>To enable accurate depreciation charges it is important that created asset classes reflect the type of assets maintained by the entity. For example, instead of creating an Information Technology asset class, asset classes should be created for different types of computer equipment including computers, routers, etc.</td>
</tr>
<tr>
<td>Segregate the ability to maintain asset</td>
<td>The ability to purchase an asset through Accounts Payable or Purchasing should be segregated from the ability to maintain asset records to reduce the risk that assets can be misappropriated.</td>
</tr>
<tr>
<td>records and purchase assets</td>
<td></td>
</tr>
</tbody>
</table>
8.2 Asset Transaction Postings

Functional overview

Asset transaction postings including acquisitions, retirements and revaluations impact on the new book value of the asset balance within the General Ledger.

Asset transaction postings include:

- Asset acquisitions.
  - There are four different types of asset acquisitions: purchase acquisition; acquisition from in-house production; subsequent acquisition to an already capitalised asset; and post capitalisation.
- Asset terminations.
- Depreciation postings.
- Asset transfers between locations and cost centres.
- Asset revaluations.

Asset depreciation overview
Commonly identified control weaknesses

The following control weaknesses typically occur in Asset Accounting implementations:

<table>
<thead>
<tr>
<th>Control weakness</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capitalisation of purchased assets</td>
<td>Assets can be created / capitalised into Asset Accounting through Accounts Payable, Purchasing or through the Project System. Often there are problems with entity's capitalisation policies and configuration, resulting in incorrect recording of asset values.</td>
</tr>
</tbody>
</table>
| Incorrect allocation of planned useful life values to asset classes | Depreciation charges are calculated based on the useful life and depreciation method allocated to each asset record. Often incorrect depreciation charges can be recorded to the General Ledger because of problems that occur with useful life allocations including:  
  • Asset records may be allocated to an incorrect asset class.  
  • Incorrect allocation of useful life values to asset class records.  
  • It is possible for staff processing asset records to override asset useful life records. Failure to define minimum and maximum useful lives on asset records can result in incorrect depreciation rates.|

Summary of risks

- **High**
  - Asset depreciation charges are incorrect
  - Expenditure is not correctly capitalised
  - Asset acquisitions are not approved
  - Failure to record all asset acquisitions within the General Ledger

- **Medium**
  - Asset retirements and transfers are processed incorrectly.
  - Asset revaluations are incorrectly performed

- **Segregation of duties risks**
  - Asset Master Record Maintenance and Asset Transactions
## Risks and controls

<table>
<thead>
<tr>
<th>R803: Asset depreciation charges are incorrect</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk rating</strong></td>
</tr>
<tr>
<td><strong>Risk description</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Controls</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
R803: Asset depreciation charges are incorrect (continued)

**Manual controls**

*Establishment of chart of depreciation and depreciation areas*
It is important that the chart of depreciation and depreciation areas have been adequately established. Any changes to depreciation rates should be adequately approved. As an example any changes to tax rates should be approved by the tax accountants. (C1040)

*Documented procedures*
Formal detailed procedures which document the process for acquiring, maintaining, transferring and disposing of fixed assets should be in place. These procedures should detail the use of any supporting documentation which is required along with details of the transaction and the staff that are allowed to authorise asset transactions. A periodic check of supporting documentation can then be performed to the reports produced by the system. (C1041)

*Policy for allocating asset classes*
A policy should be implemented to describe how assets should be allocated to classes in order to reduce the likelihood of assets being allocated to an incorrect asset class. This should include a precise definition of low value asset records. (C1042)

*Maintenance of asset posting periods*
Asset posting periods should be maintained to ensure that only the current period is open for posting to prevent depreciation from being posted to the wrong accounting period. (C811)

*End-of-month procedures*
Detailed procedures should be in place outlining end-of-month procedures. This will include the processing of depreciation posting and subsequent correction of any errors which may occur. Also included should be the review of key reports to ensure that monthly depreciation charges appear to be reasonable. (C1043)

Transaction code AR14 should be used to review all manual depreciation charges. (C367)
R804: Expenditure is not correctly capitalised

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>A key financial statement risk is that expenditure is incorrectly expensed instead of being capitalised into the Asset Management module. It is important that SAP is configured effectively to allocate capitalised expenditure through either the Accounts Payable or Purchasing processes.</td>
</tr>
<tr>
<td>Controls</td>
<td>Configuration controls</td>
</tr>
</tbody>
</table>

SAP provides the ability to automatically capitalise assets when purchased through Purchasing using Purchase Order transactions ME21 or ME21N. To enable this automation, the capitalisation flag should be set for key transaction types. When the capitalisation flag is set, assets are automatically created when an invoice is matched to its related purchase order in Accounts Payable or where an invoice is processed directly as an accounting document. (C347) (C371)

**Improving the accuracy of depreciation charges using Asset Class Useful Life configuration controls**

The asset module of SAP is driven by asset class. When an asset is created it is allocated an asset class. The useful life and depreciation key allocated to the asset class for the relevant depreciation area is then defaulted for the asset. It is, therefore, important that Asset Class configuration is correct to ensure depreciation calculations and the financial statements are correct.

Often entities will allocate useful life values to each of their asset classes, however asset clerks may incorrectly override the planned useful life values.

To address these problems, the following two key controls are suggested to ensure that the useful life allocated to an asset is correct:

- Each asset class should be set up with an appropriate planned useful life, which was defaulted when the asset is created.
- Since the planned useful life can be overwritten during asset creation, each asset class should have a maximum and minimum useful life allocated.

Source: Protiviti Australia
## R805: Acquisitions are not approved

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Asset acquisitions are acquired without appropriate approvals resulting in potential misappropriation of attractive asset items.</td>
</tr>
</tbody>
</table>

### Controls

**Manual controls**

*Approving of asset acquisitions*

All asset acquisitions should be approved either through Purchasing via purchasing release strategies or through capital purchase programs. Approvals should be processed against the entities delegations of authorities. A standard fixed asset creation form is typically used for recording and authorising assets. (C349)

## R806: Failure to record all asset transactions within the General Ledger

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Asset acquisitions, depreciation and retirement values must be sent to the General Ledger for financial statement purposes. Incorrect configuration of Asset Accounting and General Ledger integration settings can result in financial statement misstatements.</td>
</tr>
</tbody>
</table>

### Controls

**Configuration controls**

*Depreciation areas post to the General Ledger*

It is possible to configure whether depreciation areas (such as 01 book depreciation) post to the General Ledger. At a minimum, all book depreciation areas should post to the General Ledger. (C350)

*Appropriate General Ledger accounts*

An appropriate General Ledger account must be allocated to each asset class to enable adequate recording of current and non current assets. (C694)

*Asset reconciliation report*

Included within the implementation guide is an asset reconciliation report which analyses the asset system and compares detail to the General Ledger. (C506)

**Manual controls**

*Reconciling procedures*

Procedures should be in place for the fixed assets sub-ledger to be periodically reconciled to the fixed assets control accounts in the general ledger. This will assist in verifying the accuracy of General Ledger postings. (C1044)
### R807: Asset retirements and transfers are processed incorrectly

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
</table>
| Risk description | Failure to account for asset movements, either retirements or transfers, can result in an incomplete asset register impacting the integrity of the financial statements. Key impacts include:  
  - Asset retirements are identified and processed within SAP including the correct allocation of proceeds of sale into the General Ledger.  
  - Asset movements are not identified, authorised or correctly entered.  
  - Proceeds on sales of assets are adequately reflected and recorded. |

<table>
<thead>
<tr>
<th>Controls</th>
<th>Configuration controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Setting up asset retirement transaction types</strong></td>
</tr>
<tr>
<td></td>
<td>Asset retirement transaction types should be appropriately set up to ensure that the system logs an asset retirement date and changes the status of the asset to ‘retired’ to prevent the asset from being subject to further processing. (C516)</td>
</tr>
<tr>
<td></td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td><strong>Periodic review of audit trail</strong></td>
</tr>
<tr>
<td></td>
<td>An audit trail of changes to assets can be periodically reviewed. Alternatively, cost centre owners should periodically review reports of the assets which belong to their cost centres to ensure that changes have been authorised. (C1045)</td>
</tr>
<tr>
<td></td>
<td><strong>Documenting and authorising of all asset retirements</strong></td>
</tr>
<tr>
<td></td>
<td>All asset retirements should be recorded on a standard form and be appropriately authorised. (C1046)</td>
</tr>
<tr>
<td></td>
<td><strong>Periodic review of Asset Retirements Report</strong></td>
</tr>
<tr>
<td></td>
<td>The Asset Retirements Report, RAAEND02, transaction code AR16, should be periodically reviewed to ensure that all asset retirements have been authorised and accurately processed in the system and profit or loss on sale is adequately recorded. (C358)</td>
</tr>
<tr>
<td></td>
<td><strong>Periodic review of Asset Transfers Report</strong></td>
</tr>
<tr>
<td></td>
<td>The Asset Transfers Report RAUMBU_ALV01, transaction code S_ALR_87012054, should be periodically reviewed to ensure that all asset transfers have been authorised and accurately processed in the system. (C1047)</td>
</tr>
</tbody>
</table>
R808: Asset revaluations are incorrectly performed

<table>
<thead>
<tr>
<th>Risk rating</th>
<th>MEDIUM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk description</td>
<td>Assets are incorrectly revalued, resulting in an incorrect book value recorded against the asset.</td>
</tr>
<tr>
<td>Controls</td>
<td>Manual controls</td>
</tr>
</tbody>
</table>

**Accounting standards and expert advice**
Revaluations should be performed in accordance with the accounting standards. Revaluations should be performed in accordance with expert advice whenever possible. (C359)

Security considerations

Transactions of which access should be restricted to relevant Finance/Asset Accounting staff

<table>
<thead>
<tr>
<th>Security Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transactions</td>
<td></td>
</tr>
<tr>
<td>AB01</td>
<td>Create Asset Transaction</td>
</tr>
<tr>
<td>AB02</td>
<td>Change Asset Document</td>
</tr>
<tr>
<td>ABAA</td>
<td>Unplanned Depreciation</td>
</tr>
<tr>
<td>ABAO, ABAON</td>
<td>Asset Sale without customer</td>
</tr>
<tr>
<td>AFAB, AFABN</td>
<td>Post Depreciation</td>
</tr>
<tr>
<td>F-91</td>
<td>Asset acquisition posted with clearing account</td>
</tr>
<tr>
<td>F-92</td>
<td>Asset acquisition from sale with customer.</td>
</tr>
<tr>
<td>AW01, AW01N</td>
<td>Asset Explorer(reporting)</td>
</tr>
<tr>
<td>Authorisation Objects</td>
<td></td>
</tr>
<tr>
<td>A_B_ANLKL</td>
<td>Asset Account posting by asset class</td>
</tr>
<tr>
<td>A_PERI_BUK</td>
<td>Specific processing activities in Asset Accounting</td>
</tr>
<tr>
<td>F_BKPF_BUK</td>
<td>Accounting Document by Company Code</td>
</tr>
<tr>
<td>F_BKPF_KOA</td>
<td>Accounting Document by application</td>
</tr>
</tbody>
</table>
Common segregation of duties areas of concern

<table>
<thead>
<tr>
<th>Function 1</th>
<th>Function 2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Master Record Maintenance</td>
<td>Asset Transactions</td>
<td>A user with the ability to maintain Asset Master Records and process asset transactions which including acquisitions, retirements and depreciation actions, could perform a number of inappropriate actions including writing off and misappropriating assets, retiring assets without revenue and performing inappropriate depreciation activities which can impact the financial statements.</td>
</tr>
</tbody>
</table>

Optimising the SAP control environment

- Set minimum and maximum values on asset records

Better practice items to consider in the use of Asset Accounting include:

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set minimum and maximum values on asset records</td>
<td>Although the useful life value on asset class records is defaulted when an asset record is created, there is a risk that the useful life value can be overridden when creating the asset. Within SAP configuration a minimum and maximum useful life should be set for all asset classes to control the extent of change to the planned useful life.</td>
</tr>
</tbody>
</table>
Appendices

Appendix 1: Terminology and definitions 247
Appendix 2: Upgrading to ECC 265
Appendix 3: SAP and segregation of duties risks 267
## Appendix 1: Terminology and definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABAP reports</td>
<td>Reports generated using ABAP.</td>
</tr>
<tr>
<td>ABAP/4</td>
<td>Advanced Business Application Programming. The proprietary fourth generation SAP programming language.</td>
</tr>
<tr>
<td>Access control</td>
<td>The process of restricting access to particular SAP areas, transactions or functions to authorised users.</td>
</tr>
<tr>
<td>Account assignment / account</td>
<td>A process whereby the general ledger accounts are updated as a result of a transaction entered by the user or automatically determined by the system based on parameters which have been set up during system implementation.</td>
</tr>
<tr>
<td>determination</td>
<td></td>
</tr>
<tr>
<td>Account group</td>
<td>An account group is a master data structure that is used to group similar master records (e.g. vendors). It controls the number range used for the master record as well as key control data such as the data entry characteristics.</td>
</tr>
<tr>
<td>Account type</td>
<td>The type of account which can be general ledger, customer, vendor, asset, or material. It determines which general ledger accounts can be posted to.</td>
</tr>
<tr>
<td>Activation</td>
<td>The process of preparing a profile/authorisation for use. When a profile/authorisation is maintained, it is saved as an ‘update’ version. It must then be activated in order to be used in the system (this is referred to as the ‘active’ version).</td>
</tr>
<tr>
<td>Activities</td>
<td>Referring to Project System, activities are the key tasks to be completed. Activities map to internal activities, external activities, cost activities and materials components. Also refer to Work Breakdown Structure.</td>
</tr>
<tr>
<td>Activity group</td>
<td>An activity group is a collection of tasks in the system that are performed for a given user role.</td>
</tr>
<tr>
<td>Activity-based accounting</td>
<td>Component of controlling that allows additional capabilities for allocating costs to products based on the cross-departmental processes performed by the entity.</td>
</tr>
<tr>
<td>ALE (Application Linking and</td>
<td>Technology that allows for the integration of business processes between SAP systems, taking into account how distributed among the different components of SAP they are. It can also facilitate the integration of business processes between SAP systems and non-SAP systems.</td>
</tr>
<tr>
<td>Enabling) landscape</td>
<td></td>
</tr>
<tr>
<td>Application server</td>
<td>The computer which performs the application processing for the SAP system.</td>
</tr>
<tr>
<td>Asset accounting</td>
<td>Component of SAP that is used for managing and supervising fixed assets.</td>
</tr>
<tr>
<td>Asset class</td>
<td>The asset class is the primary criterion used for classifying assets. Each asset must belong to only one asset class.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Asset master</td>
<td>Used for recording the master data of an entity’s fixed assets on an individual asset basis.</td>
</tr>
<tr>
<td>Audit trail</td>
<td>Tracking and recording the details of a particular transaction or activity.</td>
</tr>
<tr>
<td>Australian Government</td>
<td>A manual that provides an ICT security framework that enables entities to meet their business obligations while considering the risk environment. Further information may be found at <a href="http://www.dsd.gov.au/library/infosec/acsi33.html">http://www.dsd.gov.au/library/infosec/acsi33.html</a></td>
</tr>
<tr>
<td>Information and</td>
<td></td>
</tr>
<tr>
<td>Communications</td>
<td></td>
</tr>
<tr>
<td>Technology Security</td>
<td></td>
</tr>
<tr>
<td>Manual (ISM)</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>Verifying the identity of a particular user undertaking a particular activity (i.e. whether a user logging onto the system is authorised to do so).</td>
</tr>
<tr>
<td>Authorisation</td>
<td>Defines an access right for an individual authorisation object (i.e. assigns values for the fields in the object). Authorisations are grouped together to form profiles which are in turn assigned to users.</td>
</tr>
<tr>
<td>Authorisation group</td>
<td>An authorisation group is a group that can be defined to restrict access to executing/maintaining programs in SAP. An authorisation group can be allocated for each program and users can then be given access to perform functions for specific authorisation groups only.</td>
</tr>
<tr>
<td>Authorisation objects</td>
<td>The foundation of SAP security. Objects serve as a template for coding access checks in ABAP programs and for establishing user access rights. When values are defined for authorisation objects these are referred to as authorisations.</td>
</tr>
<tr>
<td>Background processing</td>
<td>Processing which is performed by the system in the background. At the same time the user is able to continue processing other online tasks/functions while the background job is running.</td>
</tr>
<tr>
<td>Basis</td>
<td>Includes client/server architecture and configuration, a relational database management system and a graphical user interface. In addition to the interface between system elements, the Basis component includes a development environment for SAP ERP applications and a data dictionary, as well as user and system administration and monitoring.</td>
</tr>
<tr>
<td>Blanket purchase order</td>
<td>A purchase order created with a value limit and a validity period instead of a delivery date.</td>
</tr>
<tr>
<td>Business area</td>
<td>An organisational structure within SAP which can be used for internal reporting purposes (e.g. administration).</td>
</tr>
<tr>
<td>Business continuity plan</td>
<td>A collection of procedures and information that is developed, compiled and maintained in readiness for use in a business disruption event.</td>
</tr>
<tr>
<td>CAT</td>
<td>See Cross-Application Timesheet.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Catalogue</td>
<td>A component of SRM that allows a user to browse through products online and select the products they need and the required quantities, putting this information into a user’s Shopping Cart.</td>
</tr>
<tr>
<td>Central User Administration (CUA)</td>
<td>A SAP add-on designed to address the difficulties of maintaining user accounts.</td>
</tr>
<tr>
<td></td>
<td>A system group includes several SAP systems with several clients. The same users are often created and the same roles assigned in each client. CUA is designed to perform these tasks in a central system and distribute the data to the systems in the system group.</td>
</tr>
<tr>
<td>Central user management</td>
<td>Administration of a whole system landscape from one single central system.</td>
</tr>
<tr>
<td></td>
<td>Allows overview over all user data in the whole system landscape.</td>
</tr>
<tr>
<td>Change control process</td>
<td>A process whereby changes to programs and other objects in the system are managed. Refer to Connection and Transport System (CTS).</td>
</tr>
<tr>
<td>Change management</td>
<td>The process of authorising and appropriately testing significant system changes. Includes procedures that should be followed when changes are made to an existing system. This includes requests, approvals and testing required from the relevant stakeholders throughout development to implementation.</td>
</tr>
<tr>
<td>Clearing</td>
<td>The process of receiving payment on a customer account and ‘clearing’ the payment against the outstanding accounts receivable invoice. Clearing may also refer to the process of making a payment to a vendor and clearing the payment against the outstanding accounts payable invoice.</td>
</tr>
<tr>
<td>Client</td>
<td>The highest level in the SAP organisational structure. The client would usually represent the entire entity or a group of companies. Individual organisations (or entities) or subsidiaries are represented by separate ‘company codes’ (or separate legal entities) within the client.</td>
</tr>
<tr>
<td>Client copy</td>
<td>The act of copying objects from one client to another client. This can be done within the one SAP environment (e.g. development), or from one SAP environment to another, (e.g. from development to test).</td>
</tr>
<tr>
<td>Client/server</td>
<td>A computer system where the processing is shared across different computers connected by a network. Processing is shared between the servers (in SAP processing is split across the database and application servers) and the clients (the PCs on the users’ desk).</td>
</tr>
<tr>
<td>CO</td>
<td>See Controlling module.</td>
</tr>
<tr>
<td>Commonly identified control weaknesses</td>
<td>Areas of SAP vulnerable to significant risks that require controls to address.</td>
</tr>
<tr>
<td>Component</td>
<td>Distinct part of a larger program.</td>
</tr>
<tr>
<td>Composite role</td>
<td>Collection of roles.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration</td>
<td>The act of setting parameters in the system to control the business processes performed. The system must be configured to meet the needs of the entity before it can be used.</td>
</tr>
<tr>
<td>Configuration elements (System Setting)</td>
<td>Establishing an enterprise’s own processes/functions, as defined in the conceptual design, in the SAP ERP System by configuring Customising objects</td>
</tr>
<tr>
<td>Configuration parameter</td>
<td>A setting that must be configured within a certain range.</td>
</tr>
<tr>
<td>Control environment</td>
<td>The SAP environment that requires the use of controls</td>
</tr>
<tr>
<td>Control objectives</td>
<td>Control objectives are high level statements by management that provide a link between organisational risks and the internal controls and activities implemented by entities to mitigate such risks.</td>
</tr>
<tr>
<td>Controller</td>
<td>An FF role — also known as Owner. The GRC RAR Security Role is /VRSA/Z_VFAT_ID_OWNER.</td>
</tr>
<tr>
<td>Controlling (CO) module</td>
<td>The Controlling (CO) module is primarily used for management reporting purposes. Its central function is to report exclusively on revenues and costs.</td>
</tr>
<tr>
<td>Controls</td>
<td>Policies, procedures and practices designed to mitigate and reduce the chance of risks being realised.</td>
</tr>
<tr>
<td>Correction and transport system (CTS)</td>
<td>The mechanism used for moving objects (programs, tables, configuration, data) between SAP environments.</td>
</tr>
<tr>
<td>Cost centre</td>
<td>Organisational unit within a controlling area that represents a defined location of cost incurrence. The definition can be based on: Functional Requirements, Allocation criteria, Physical location and Responsibility for costs</td>
</tr>
<tr>
<td>Cost Centre Accounting</td>
<td>Component of Controlling that allows the display of costs incurred by the business, as allocated to cost centres. Cost centres can be created for functional areas such as marketing.</td>
</tr>
<tr>
<td>Cost Element Accounting</td>
<td>Component of Controlling that allows the user to view an overview of the costs and revenues that occur in an entity with actual data directly from Financial Accounting.</td>
</tr>
<tr>
<td>Cross Application</td>
<td>Refers to all data objects (tables, entities or processes) that relate to more than one business application</td>
</tr>
<tr>
<td>Cross Application Timesheet (CAT)</td>
<td>Timesheet that relates to more than one business application.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cross-Talk</td>
<td>The underlying principle of SAP security where an authorisation with the greater level of access will override lower level access granted in another authorisation</td>
</tr>
<tr>
<td>CTS</td>
<td>See Correction and transport system.</td>
</tr>
<tr>
<td>CTS tables</td>
<td>The correction and transport system requires configuration to be set up to enable it to work. This configuration is stored in the CTS tables.</td>
</tr>
<tr>
<td>CUA</td>
<td>See Central User Administration.</td>
</tr>
<tr>
<td>Customising</td>
<td>Adjusting a particular aspect of SAP, or creating a custom add-on for SAP (e.g. using ABAP), that addresses the specific needs of the particular entity using SAP.</td>
</tr>
<tr>
<td>Cycle counting</td>
<td>A method of managing physical inventory whereby inventory is counted at regular intervals within a fiscal year.</td>
</tr>
<tr>
<td>Data</td>
<td>Representation of facts, concepts or instructions in a formalised manner suitable for communication, interpreting or processing by users or by automatic means.</td>
</tr>
<tr>
<td>Data classification</td>
<td>The process of classifying data as a particular data type.</td>
</tr>
<tr>
<td>Data dictionary</td>
<td>The data dictionary is used to store information centrally about the entity’s data. It controls the relationships between the data and how the data is used in programs and screens.</td>
</tr>
<tr>
<td>Database management system (DBMS)</td>
<td>Database management system. Software which is used to manage the SAP database (e.g Oracle, Informix).</td>
</tr>
<tr>
<td>DBMS</td>
<td>See Database Management System.</td>
</tr>
<tr>
<td>DDIC</td>
<td>A standard SAP user which is the only user allowed to access the SAP system during an upgrade. This user has access to all functions within the SAP system. Some of these access rights are hard-coded and therefore DDIC should not be deleted. DDIC is a powerful standard user and is therefore a target for hackers so that steps need to be taken to ensure that it is secured.</td>
</tr>
<tr>
<td>Default setting</td>
<td>The configuration settings that are in place upon installation of SAP.</td>
</tr>
<tr>
<td>Deliverables</td>
<td>The product or service that results from the completion of a project.</td>
</tr>
<tr>
<td>Derived roles</td>
<td>A derived role inherits the menu structure and functions of the referred role.</td>
</tr>
<tr>
<td>Developer key</td>
<td>The developer key is a combination of the installation number, license key and user name. The key is required for each person that will make changes in the SAP system.</td>
</tr>
<tr>
<td>Development objects</td>
<td>A modification to standard SAP or the introduction of new functionality. Generally these will be in the form of changes to a program or a new program.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disaster Recovery Plan (DRP)</td>
<td>A plan which outlines the steps which are required to recover the business systems in the event of a disaster. A disaster includes all events which may lead to the total loss of the system including fire, floods, and sabotage.</td>
</tr>
<tr>
<td>Document</td>
<td>Every transaction in the SAP system is called a ‘document’. All documents consist of a document header (contains general information such as company code, date, currency) and document line items (contain information such as accounts, amounts).</td>
</tr>
<tr>
<td>Document splitting</td>
<td>Document splitting enables a complex display of documents</td>
</tr>
<tr>
<td>Document type</td>
<td>Determines the type of transaction being processed. Document type controls number ranges used for posting and also determines what type of account can be posted for a given transaction (e.g., a vendor document type can only be posted against vendor accounts).</td>
</tr>
<tr>
<td>Double approval</td>
<td>The process of requiring two users, rather than one, to approve a particular item (e.g., a purchase).</td>
</tr>
<tr>
<td>DRP</td>
<td>See Disaster Recovery Plan.</td>
</tr>
<tr>
<td>Duplicate employees</td>
<td>An employee who is listed two or more times on the payroll.</td>
</tr>
<tr>
<td>Duplicate invoice check</td>
<td>A configurations setting within SAP that, when turned on, provides the user with a warning whenever the invoice about to be processed is potentially a duplicate.</td>
</tr>
<tr>
<td>Duplicate payments</td>
<td>Paying employees more than required; for example, as a result of duplicate employees on the payroll.</td>
</tr>
<tr>
<td>ECC</td>
<td>ERP central component.</td>
</tr>
<tr>
<td>ECC6</td>
<td>See SAP ECC 6.0</td>
</tr>
<tr>
<td>EFT</td>
<td>See Electronic Funds Transfer.</td>
</tr>
<tr>
<td>Electronic Funds Transfer</td>
<td>A facility that allows payments to be made electronically, as opposed to manually.</td>
</tr>
<tr>
<td>Emergency change</td>
<td>A change to the system that must be made immediately to alleviate a risk that may have a large negative impact on the system.</td>
</tr>
<tr>
<td>Emergency repairs</td>
<td>Repairs to the system in response to an emergency change.</td>
</tr>
<tr>
<td>Employee Self Service (ESS)</td>
<td>A component of the SAP HR module, the self service module allows employees to maintain their time sheet, leave requests, personal information, and display of pay slips.</td>
</tr>
<tr>
<td>Enterprise Buyer</td>
<td>See Supplier Relationship Management.</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERS</td>
<td>See <em>Evaluated receipts settlement</em>.</td>
</tr>
<tr>
<td>ESS</td>
<td>See <em>Employee Self Service</em>.</td>
</tr>
<tr>
<td>Evaluated receipts settlement (ERS)</td>
<td>Evaluated receipts settlement is the process by which suppliers are paid on the receipt of goods without the need for a separate invoice to be received.</td>
</tr>
<tr>
<td>FF</td>
<td>See Firefighter. Also refer to Superuser Privilege Management.</td>
</tr>
<tr>
<td>Fl</td>
<td>See Financial (FI) accounting module.</td>
</tr>
<tr>
<td>Field</td>
<td>A particular characteristic of a particular item that can be input/modified by a user.</td>
</tr>
<tr>
<td>Field status</td>
<td>Refers to the data entry option of an individual field.</td>
</tr>
<tr>
<td>Financial (FI) accounting module</td>
<td>This module consists of several components including general ledger, accounts receivable, accounts payable, assets accounting, legal consolidation and special ledger.</td>
</tr>
<tr>
<td>Financial Management Act (FMA Act)</td>
<td>An Act designed to provide a framework for the proper management of public money and public property.</td>
</tr>
<tr>
<td>Financial Management Information System (FMIS)</td>
<td>The information system that supports an entity’s FI function.</td>
</tr>
<tr>
<td>Firefighter</td>
<td>A user with the ability to address a common audit issue that arises when users have privileged access to the SAP production system.</td>
</tr>
<tr>
<td>Firefighter Controller</td>
<td>Users who monitor FirefightID usage by reviewing the Firefighter Log and receiving notifications of FirefightID logain events.</td>
</tr>
<tr>
<td>Firefighter Log</td>
<td>A log which keeps record of any logins and subsequent transaction usage made by Firefighters.</td>
</tr>
<tr>
<td>FirefightID</td>
<td>A specific ID given to Firefighters for a designated period of time.</td>
</tr>
<tr>
<td>FirefightID Administrator</td>
<td>Users who maintain the configuration of the Firefighter system. They assign FirefightIDs to Firefighters and Controllers.</td>
</tr>
<tr>
<td>Fraud / fraudulent activity</td>
<td>Dishonestly obtaining a benefit by deception or other means.</td>
</tr>
<tr>
<td>Function</td>
<td>A task that an employee performs to accomplish a specific portion of his/her job responsibilities. A function is a grouping of one or more relate actions and/or permissions for a specific business area. An example of a function is Vendor Maintenance. This function would include all of the SAP transactions that can be used to maintain a vendor account.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>General Ledger</td>
<td>A complete record of all business transactions. It provides a comprehensive picture for external accounting and accounts.</td>
</tr>
<tr>
<td>Ghost employees</td>
<td>Fictitious employees in the payroll system that can be used to make fraudulent payments.</td>
</tr>
<tr>
<td>Goods Receipt (GR)</td>
<td>The process of receiving and accepting goods/services.</td>
</tr>
<tr>
<td>GR/IR clearing account</td>
<td>A clearing account in the general ledger that represents the timing difference between the receipt of goods and the processing of an invoice.</td>
</tr>
<tr>
<td>Grants</td>
<td>A grant is a sum of money given to entities or individuals for a specified purpose directed at achieving goals and objectives consistent with government policy.</td>
</tr>
<tr>
<td>Grants management (SAP)</td>
<td>Part of the SAP Public Service industry solution; supports all business processes a grantee must engage in, starting with preparatory activities prior to receiving funds to the accounting and reporting activities required after grants are awarded.</td>
</tr>
<tr>
<td>Graphical user interface</td>
<td>The interface that is presented to the user (i.e. screen design and layout).</td>
</tr>
<tr>
<td>GRC</td>
<td>Governance, Risk and Compliance — refers to a solution developed by SAP.</td>
</tr>
<tr>
<td>GRC Access Control</td>
<td>Component of GRC that identifies and prevents access and authorisation risks in cross-enterprise IT systems to prevent fraud and reduce the cost of continuous compliance and control.</td>
</tr>
<tr>
<td>GRC Global Trade Management</td>
<td>Component of GRC that manages foreign trade processes to ensure trade compliance, expedited cross-border transactions and optimum utilisation of trade agreements.</td>
</tr>
<tr>
<td>GRC Process Controls</td>
<td>Component of GRC that documents business process controls and allows creation of automated process control testing routines.</td>
</tr>
<tr>
<td>GRC Risk Management</td>
<td>Component of GRC that facilitates the documentation and management of financial, legal and operational risks.</td>
</tr>
<tr>
<td>GUI</td>
<td>See Graphical User Interface.</td>
</tr>
<tr>
<td>Human Resource Management</td>
<td>The information system that supports an entity’s HR function, allowing the entity to automate tasks such as processing employee payments.</td>
</tr>
<tr>
<td>Information System (HRMIS)</td>
<td></td>
</tr>
<tr>
<td>IMG</td>
<td>See Implementation Guide</td>
</tr>
<tr>
<td>Implementation Guide SAP (IMG)</td>
<td>The implementation guide (IMG) is an online manual that is used to assist in configuring SAP. The IMG lists all activities for implementing each SAP module.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Infosystem</td>
<td>A collection of reports grouped by application area within SAP (e.g., accounts payable infosystem).</td>
</tr>
<tr>
<td>Infotype</td>
<td>Changes are performed on HR master data through groups of information called infotypes (e.g., taxation information). Infotypes are created for each master record as applicable.</td>
</tr>
<tr>
<td>Instance</td>
<td>An instance refers to a separate physical SAP database. There may be several clients on one instance. Development, Test and Production environments will ideally be located in separate instances.</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>A section within an entity that analyses the entity’s activities, processes and controls, and recommends solutions to address any areas of improvement.</td>
</tr>
<tr>
<td>Internal Order Accounting</td>
<td>Component of Controlling that allows for the tracking of costs as incurred by a specific job, service, project, or task.</td>
</tr>
<tr>
<td>Invoice processing</td>
<td>The process of matching invoices to the relevant purchase order and goods/service receipt.</td>
</tr>
<tr>
<td>Invoice receipt (IR)</td>
<td>The process of receiving invoices from vendors.</td>
</tr>
<tr>
<td>Invoice Tolerance</td>
<td>A configuration setting that allows users to ensure that significant variations between the purchase order, goods receipt and invoice are blocked.</td>
</tr>
<tr>
<td>IR</td>
<td>See Invoice Receipt</td>
</tr>
<tr>
<td>J2EE</td>
<td>A platform independent environment that can be used to develop Web-based applications.</td>
</tr>
<tr>
<td>Key element</td>
<td>An element which is particularly crucial to the component of which it pertains.</td>
</tr>
<tr>
<td>Legacy system</td>
<td>A term used to refer to the previous computer system which has been (or is being) replaced by SAP. Some legacy systems may remain in operation and data may be interfaced between these systems and SAP.</td>
</tr>
<tr>
<td>Lightweight Directory</td>
<td>An internet protocol that programs use to look up information from a server.</td>
</tr>
<tr>
<td>Access Protocol (LDAP)</td>
<td></td>
</tr>
<tr>
<td>Line item</td>
<td>Refers to the detailed portion of a document/transaction. The line item is the individual debit or credit entry.</td>
</tr>
<tr>
<td>Low value asset class</td>
<td>An asset class used to class assets of low value.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Managers Desktop</td>
<td>This component of the SAP HR module allows functional managers to perform administrative tasks within their area and access relevant HR, financial, or controlling data.</td>
</tr>
<tr>
<td>Manual cheque payment</td>
<td>Using paper based cheques to make payments.</td>
</tr>
<tr>
<td>Manual control</td>
<td>A type of control that requires manual intervention, either in combination or separate from SAP, to perform.</td>
</tr>
<tr>
<td>Material master file</td>
<td>A master file that is used to store the materials that are purchased by an entity.</td>
</tr>
<tr>
<td>Materials requirement planning (MRP)</td>
<td>Procedures within the materials management/logistics modules of SAP which are used to determine the future requirements for materials that are required to fulfil customer orders. The system can be configured to automatically order the required materials without user intervention.</td>
</tr>
<tr>
<td>Minimum password length</td>
<td>The minimum amount of characters a password must contain in order to be used as a password within SAP.</td>
</tr>
<tr>
<td>Mitigating control</td>
<td>A control designed to decrease or offset the chance of a particular risk being realised. Also a term used in GRC.</td>
</tr>
<tr>
<td>Movement type</td>
<td>Determines the type of inventory movement recognised by SAP and the corresponding accounting, including which quantity fields, stock types and general ledger accounts are updated</td>
</tr>
<tr>
<td>Moving average price</td>
<td>A material price that is updated after each purchasing transaction by determining the overall average price of the purchased material.</td>
</tr>
<tr>
<td>Negative postings</td>
<td>The non-preferred action of making a negative posting to reverse a transaction, as opposed to the preferred action of reversing the original transaction.</td>
</tr>
<tr>
<td>NetWeaver</td>
<td>A set of tools and technologies that provide users with a unified interface between Java and ABAP based SAP systems.</td>
</tr>
<tr>
<td>NetWeaver administrator (NWA)</td>
<td>The central point for the administration, configuration and monitoring for the various SAP and non-SAP components that are managed by NetWeaver.</td>
</tr>
<tr>
<td>Networks</td>
<td>A list of tasks organised into a process flow with specific timing. Derived from WBSs.</td>
</tr>
<tr>
<td>New General Ledger</td>
<td>A New General Ledger component introduced within ECC5/ECC6. Entities can choose to implement either this or the traditional General Ledger component.</td>
</tr>
<tr>
<td>No approval</td>
<td>An item that requires no approval prior to release.</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Ensuring that the validity of something (e.g. a user account) cannot be disputed.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number range</td>
<td>A range of numbers which are allocated for assignment to a particular transaction type within SAP. Every transaction/document within SAP is assigned a unique number. It is important to ensure that document number ranges do not overlap.</td>
</tr>
<tr>
<td>OCR</td>
<td>See Optical character recognition.</td>
</tr>
<tr>
<td>One-time vendor account (OTV)</td>
<td>One-time vendor accounts are used for vendors from whom goods are expected to be purchased only once. It permits entry of the vendor name, address and bank details in the invoice. A vendor master record is not established for the individual vendor.</td>
</tr>
<tr>
<td>Online Support Service (OSS)</td>
<td>A service offered by SAP which enables technical staff to log onto a SAP system in Germany to retrieve information about upgrades and fixes/enhancements for problems with the system. SAP is also able to access the entity’s system via the OSS utility to provide analysis services.</td>
</tr>
<tr>
<td>Operating system</td>
<td>The software used to control the operation of the computer system (e.g. UNIX, Windows NT).</td>
</tr>
<tr>
<td>Optical character recognition (OCR)</td>
<td>Technology that can capture an image for identification purposes.</td>
</tr>
<tr>
<td>Optimising SAP controls</td>
<td>Practices that, if adopted by an entity, would strengthen its internal control framework and lead to improved operational effectiveness and efficiency.</td>
</tr>
<tr>
<td>Entity splits</td>
<td>Within SAP, each entity has a distinct set of organisational parameters defined for it, including company codes, plant, sales and purchasing entities and personnel areas. Access to each of these entity parameters can be restricted through various SAP security authorisation objects. Entity splits means restricting access to different elements of the entity. This is done within SAP using one of the entity elements like company code, plant location, sales or purchasing entity.</td>
</tr>
<tr>
<td>Entity structure</td>
<td>The hierarchy of the entity, including the assigning of employees to positions.</td>
</tr>
<tr>
<td>OSS</td>
<td>See Online Support Service.</td>
</tr>
<tr>
<td>Outline agreement</td>
<td>The general term for a contract or a scheduling agreement. These are long term agreements with a supplier which are set up in SAP.</td>
</tr>
<tr>
<td>Owner</td>
<td>An FF role – also known as Controller. The GRC RAR Security Role is /VIRSA/Z_VFAT_ID_OWNER.</td>
</tr>
<tr>
<td>Parked journals</td>
<td>Journals that have outstanding items or questions.</td>
</tr>
<tr>
<td>Patches and OSS notes</td>
<td>Occasionally a “bug” will be discovered in SAP. These can often be fixed by checking on OSS (Online service system) for notes about how to fix the bug. These repairs are also known as patches.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Payment methods</td>
<td>The method of payment (eg cheque, electronic funds transfer).</td>
</tr>
<tr>
<td>Payment processing</td>
<td>The process of paying the vendor and claiming prompt payment discounts as a result of payment terms.</td>
</tr>
<tr>
<td>Payment terms</td>
<td>The discount an entity can receive on goods/services should they pay the vendor by a certain time set by the vendor (e.g. a three per cent discount if paid within 10 days).</td>
</tr>
<tr>
<td>Payroll Accounting</td>
<td>A component of the SAP HR module that provides a number of work processes including the generation of payroll results and remuneration statements, bank transfers and cheque payments.</td>
</tr>
<tr>
<td>Payroll Calculation</td>
<td>Function under Payroll Accounting that involves the process of performing the periodic calculation of employee costs, calculation of leave accrual balances and updating these amounts in the financial records of the entity.</td>
</tr>
<tr>
<td>Payroll Payment</td>
<td>Function under Payroll Accounting that involves the process of approving the payroll calculation for payments to employees and processing the physical payment to the employees, banks, and various vendors.</td>
</tr>
<tr>
<td>Personal Time Management</td>
<td>A component of the SAP HR module that is used in the planning, recording and valuation of employees’ work performed and absence times.</td>
</tr>
<tr>
<td>Personnel Management</td>
<td>A component of the SAP HR module that is used for maintaining employee/organisational master data, processing employee hiring and termination, performing organisational planning, budgeting and recruitment, and administering salaries, benefits and expenses.</td>
</tr>
<tr>
<td>Plant</td>
<td>An organisational structure used within the SAP materials management module. A plant may correspond to an individual warehouse/plant/location within the entity. A user’s access can be restricted to specific plants.</td>
</tr>
<tr>
<td>Posting date</td>
<td>The date which a transaction is actually posted to the general ledger. This is controlled by the availability of the posting period.</td>
</tr>
<tr>
<td>Posting key</td>
<td>A two-digit code used to determine whether a line item entry is a debit or credit. It also determines the type of general ledger account that can be posted (e.g. vendor accounts) as well as the data entry characteristics (e.g. which fields are required).</td>
</tr>
<tr>
<td>Procurement</td>
<td>The process of acquiring properties or services.</td>
</tr>
<tr>
<td>Product Cost Controlling</td>
<td>Component of Controlling that allows for the calculation of the costs of the product being manufactured or the service provisioned.</td>
</tr>
<tr>
<td>Profile</td>
<td>A collection of authorizations which have been grouped together to be allocated to a user (to assign access capabilities).</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Profile generator</td>
<td>A tool used to automate the creation of profiles based on menu functions. Refer Appendix 1.</td>
</tr>
<tr>
<td>Profit Centre Accounting</td>
<td>Component of Controlling that allows for the evaluation of profit and loss for individual profit centres.</td>
</tr>
<tr>
<td>Profitability Analysis</td>
<td>Component of Controlling that allows for the calculation of operating profit and contribution margins by individual market segments.</td>
</tr>
<tr>
<td>Project System</td>
<td>SAP module that optimises the business processes from project planning through to completion and enables project monitoring.</td>
</tr>
<tr>
<td>Purchase order</td>
<td>An order placed with a vendor for specified quantities of products at a particular price.</td>
</tr>
<tr>
<td>Purchase requisition</td>
<td>A request to acquire a defined quantity of specified products.</td>
</tr>
<tr>
<td>Purchasing Approver</td>
<td>SAP user whose role it is to approve purchase documents.</td>
</tr>
<tr>
<td>Purchasing Document Creator</td>
<td>SAP user whose role it is to create purchase documents.</td>
</tr>
<tr>
<td>Purchasing documents</td>
<td>SAP terminology for documents used in the purchasing process including purchase requisition and purchase order.</td>
</tr>
<tr>
<td>Purchasing info record</td>
<td>An info record is used by SAP to store information relating to purchasing. It is used to store information about various materials and the vendors who supply the various materials.</td>
</tr>
<tr>
<td>Purchasing value keys</td>
<td>Used to assign a number of default settings (e.g., delivery tolerances) to material master records.</td>
</tr>
<tr>
<td>Quotation</td>
<td>A document sent by a vendor to the proposed purchaser detailing the proposed cost of the good/service requested by the purchaser.</td>
</tr>
<tr>
<td>RAR</td>
<td>See Risk Analysis and Remediation</td>
</tr>
<tr>
<td>Real-time</td>
<td>Refers to the process where tasks in the SAP system are performed and the database updated immediately.</td>
</tr>
<tr>
<td>Recommended setting</td>
<td>Configuration settings which are recommended which may or may not be the same as the default settings. If different from default settings then configuration settings must be changed to reflect the recommended setting.</td>
</tr>
<tr>
<td>Reconciliation account</td>
<td>A control account which is used to record the total of all sub-ledger entries in the general ledger (e.g., the total of all postings to the vendors sub-ledger is summarised in the one control/reconciliation account in the general ledger).</td>
</tr>
<tr>
<td>Release</td>
<td>The version of SAP (e.g., SAP R/3 release 3.1H). There are usually two to three new releases of SAP produced each year.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Release procedure</td>
<td>A release procedure is used to enforce the electronic authorisation of purchase requisitions/purchase orders.</td>
</tr>
<tr>
<td>Release strategy, Release strategies</td>
<td>A mechanism used to control the electronic authorisation of purchase requisitions/purchase orders based on the delegation levels/approval sequences defined for an entity.</td>
</tr>
<tr>
<td>Remediation Process</td>
<td>A process that supports RAR; includes changing the SAP security structure, modifying employees’ responsibilities and documenting mitigating controls</td>
</tr>
<tr>
<td>Repair</td>
<td>A correction/modification made to an SAP object.</td>
</tr>
<tr>
<td>Request for Quotation (RFQ)</td>
<td>Requests for potential vendors to submit a quotation.</td>
</tr>
<tr>
<td>RFQ</td>
<td>See Request for Quotation</td>
</tr>
<tr>
<td>Risk</td>
<td>A combination of the likelihood of an adverse event occurring and the consequence that such an event may have on the entity.</td>
</tr>
<tr>
<td>Risk Analysis and Remediation (RAR)</td>
<td>An automated security audit and segregation of duties analysis application used to identify, analyse and resolve all segregation of duties and security audit issues.</td>
</tr>
<tr>
<td>SAP ECC 6.0/SAP ERP</td>
<td>A large integrated data processing system. It provides the complex application software required to support the various business processes of the entity, including financial accounting and human resources.</td>
</tr>
<tr>
<td>SAP Enterprise Portal</td>
<td>A portal that allows an entity to integrate information, applications, and services on a browser-based user interface.</td>
</tr>
<tr>
<td>SAP ERP</td>
<td>A version of SAP that may be SAP ECC6.0 or a previous version. Regardless of the version, it is the central component of SAP that contains modules such as Financial Accounting and Controlling, as distinct from add-on components such as SRM.</td>
</tr>
<tr>
<td>SAP roles, SAP profiles</td>
<td>The standard security roles and profiles within SAP that may be used by the entity.</td>
</tr>
<tr>
<td>SAP*</td>
<td>SAP*[pronounced “SAP star”] is a user master record which is delivered with the standard SAP system. This user has access to all functions within the SAP system. Because it is a powerful standard user, it is a target for hackers and steps need to be taken to ensure that it is secured.</td>
</tr>
<tr>
<td>SAProuter</td>
<td>A program which is used by SAP to simplify the configuration of network security and the direction of network traffic to and from SAP.</td>
</tr>
<tr>
<td>Secure Sockets Layer (SSL)</td>
<td>An internet standard protocol used to secure communications across the internet.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security considerations</td>
<td>Configuration options within SAP that can be adjusted to minimise the chance of fraud or error.</td>
</tr>
<tr>
<td>Security monitoring</td>
<td>The process of monitoring the security surrounding the SAP system, which includes revisiting security configurations and controls on a regular basis, not just after system implementation.</td>
</tr>
<tr>
<td>Security policy</td>
<td>Security guidelines that ensure that users and IT staff are prevented from accessing programs and data.</td>
</tr>
<tr>
<td>Segregation of duties</td>
<td>A primary internal control used when undertaking financial operations, which is intended to prevent a single individual from having control over all stages of financial transactions. The objective of segregation of duties is to ensure that different people are involved in the different stages of a transaction, consisting mainly of the initiation, authorisation/approval, recording, and settlement processes.</td>
</tr>
<tr>
<td>Segregation of duties risk</td>
<td>The assigning of different users to functions that, if performed by the same user, increase the chances of fraud and/or error taking place.</td>
</tr>
<tr>
<td>Sensitive data (HR)</td>
<td>Data that has the potential to invade the privacy of the employees and/or lead to fraudulent payments if unauthorised users are able to view/modify the data (e.g. bank account details).</td>
</tr>
<tr>
<td>Sensitive employee groups</td>
<td>Particular groups of the entity that are separated from the rest to ensure the integrity and privacy of the relevant information (e.g. executives).</td>
</tr>
<tr>
<td>Sensitive fields</td>
<td>Fields that contain sensitive data/information.</td>
</tr>
<tr>
<td>Sensitive system table</td>
<td>A table produced for use in the SAP system that contains sensitive data; changes to such tables should be logged and reports should be reviewed to detect any unauthorised changes to these tables.</td>
</tr>
<tr>
<td>Service acceptance</td>
<td>The process of accepting a service from a vendor; must be segregated from Service Master Maintenance.</td>
</tr>
<tr>
<td>Service master maintenance</td>
<td>Process that involves creating and storing service master records and using them for payment for services.</td>
</tr>
<tr>
<td>Session</td>
<td>A SAP window in which the user can process tasks. SAP allows the user to have up to nine sessions open at the same time.</td>
</tr>
<tr>
<td>Settlement rules</td>
<td>The conditions that must be complied with in order to settle internal order costs.</td>
</tr>
<tr>
<td>Shared Services environments</td>
<td>Consolidating the number of SAP instances run to eliminate IT spending.</td>
</tr>
<tr>
<td>Shared Services Unit</td>
<td>The business unit or entity that is created to manage the shared services initiative.</td>
</tr>
<tr>
<td>Shopping Cart</td>
<td>A component of SRM that keeps a record of the products the user wants to purchase.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Single approval</td>
<td>The process of requiring a user to approve a particular item (e.g. a purchase).</td>
</tr>
<tr>
<td>Single sign-on</td>
<td>A mechanism that allows users to log on once for every system they log on to.</td>
</tr>
<tr>
<td>Source determination</td>
<td>The SAP system’s ability to suggest an appropriate vendor for the products being procured.</td>
</tr>
<tr>
<td>Source list</td>
<td>A list containing the possible sources of supply (i.e., vendors) for a given material/service. It can be used to assist in the selection of a vendor when purchasing specific goods/services.</td>
</tr>
<tr>
<td>Special ledger</td>
<td>A module within SAP financial accounting which is used to collate information from various other modules in the system to perform more comprehensive reporting and analysis of information.</td>
</tr>
<tr>
<td>SRM</td>
<td>See Supplier Relationship Management.</td>
</tr>
<tr>
<td>Standard SAP Menu</td>
<td>Control element that offers a user several options.</td>
</tr>
<tr>
<td>Stochastic blocking</td>
<td>In stochastic blocking, the system blocks invoices for payment at random. The higher the invoice value, the higher the probability of it being stochastically blocked.</td>
</tr>
<tr>
<td>Stock take</td>
<td>Physically counting inventory to verify that balances recorded in the system are accurate.</td>
</tr>
<tr>
<td>Structural authorisations</td>
<td>A mechanism used to restrict access to elements of the entity structure. For example, a manager’s access in the payroll security can be restricted to the employee that the manager is responsible for.</td>
</tr>
<tr>
<td>Subsidiary ledger</td>
<td>A set of General Ledger accounts that, combined, make up a single item in the General Ledger.</td>
</tr>
<tr>
<td>Super user</td>
<td>A system user with powerful (often unlimited) access privileges.</td>
</tr>
<tr>
<td>Super user Privilege Management</td>
<td>Also known as Firefighter (FF). See Firefighter.</td>
</tr>
<tr>
<td></td>
<td>Provides the ability to address a common audit issue that arises when users have privileged access to the SAP production system.</td>
</tr>
<tr>
<td>Supplier Relationship Management</td>
<td>Supplier Relationship Management (SRM) – a component of SAP that allows users to purchase predefined products from approved vendors using an online catalogue. Previously known as Enterprise Buyer.</td>
</tr>
<tr>
<td>Supplier Relationship Management</td>
<td>Supplier Relationship Management (SRM) – a component of SAP that allows users to purchase predefined products from approved vendors using an online catalogue. Previously known as Enterprise Buyer, the SRM system resides on a separate SAP installation to the core SAP system.</td>
</tr>
<tr>
<td>System parameters</td>
<td>Parameters provided by SAP that define the way the SAP system operates, particularly system logon and password maintenance functions.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System tables</td>
<td>Tables which contain data specifically relevant to system settings (eg correction and transport system tables).</td>
</tr>
<tr>
<td>Table</td>
<td>A structure used within SAP to store transaction data, basic commercial data, configuration and system parameters, organisational structure data, and calculation rules.</td>
</tr>
<tr>
<td>Table class</td>
<td>A way of grouping tables. Tables can be allocated to table classes to provide security. User access can be confined to specified table classes.</td>
</tr>
<tr>
<td>Table maintenance</td>
<td>The ability to add records to or modify existing records in a table. Access to such functions should be restricted to specifically authorised users only.</td>
</tr>
<tr>
<td>Technical upgrade</td>
<td>Involves an entity only upgrading the technology underlying the SAP system when upgrading SAP.</td>
</tr>
<tr>
<td>Traditional General Ledger</td>
<td>When implementing ECC5 or ECC6, an entity can choose to implement either the New General Ledger (see New General Ledger) or the General Ledger used prior to ECC5/ECC6, the traditional General Ledger.</td>
</tr>
<tr>
<td>Transaction</td>
<td>Various functions within SAP are referred to as transactions. Most functions can be invoked by a four character transaction code.</td>
</tr>
<tr>
<td>Transaction objects</td>
<td>The foundation of SAP security. Objects serve as a template for coding access checks in ABAP programs and for establishing user access rights. When values are defined for transaction objects these are referred to as transactions.</td>
</tr>
<tr>
<td>Transport</td>
<td>The act of moving a program or other object from one SAP environment to another. This should be done using the Correction and Transport System.</td>
</tr>
<tr>
<td>Transport Management System (TMS)</td>
<td>Centralises the configuration for the Change and Transport System (CTS) for all SAP systems.</td>
</tr>
<tr>
<td>User group</td>
<td>A method of grouping user records which is used when security administration is decentralised. This enables administration of user master records to be restricted to the relevant administrator. Note that if user groups are used to control security administration, all users should be allocated to a user group.</td>
</tr>
<tr>
<td>User Management Engine (UME)</td>
<td>User Authentication and Management in NetWeaver is performed via the User Management Engine (UME).</td>
</tr>
<tr>
<td>User master record</td>
<td>This is a record which is created in the SAP system to identify a user and allocate profiles to the user. There should be a one to one relationship between the number of users of the system and the number of user master records.</td>
</tr>
<tr>
<td>Variant</td>
<td>Refers to a set of report selection parameters which can be saved and retrieved for future use.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Vendor</td>
<td>An entity of which goods and/or services can be purchased.</td>
</tr>
<tr>
<td>Vendor master data</td>
<td>A file containing information about the agency’s vendors including name and address, terms of payment, payment information (e.g. vendor bank account). A vendor master record must be established for each vendor from whom the agency purchases goods and services.</td>
</tr>
<tr>
<td>Vendor master file</td>
<td>A master data record used to store information about each of the vendors from whom an entity purchases goods or services.</td>
</tr>
<tr>
<td>Wage types</td>
<td>A component of an employee’s remuneration which may include salary/wage, bonuses, allowances, and deductions. Wage types are used to calculate employee remuneration.</td>
</tr>
<tr>
<td>WBS</td>
<td>See Work Breakdown Structure.</td>
</tr>
<tr>
<td>Work Breakdown Structure (WBS)</td>
<td>Specific deliverables or tasks for a project or program of projects. Refer to Activities.</td>
</tr>
<tr>
<td>Work centres</td>
<td>Referring to Project System, internal activities are assigned to work centres (resources) to be completed.</td>
</tr>
<tr>
<td>Workbench organiser</td>
<td>The SAP environment where modifications can be made to ABAP programs and other system objects.</td>
</tr>
<tr>
<td>Workflow</td>
<td>A SAP utility that can be used to control the time and logical sequence in which work items are processed (e.g. workflow can be used to help automate the electronic approval of purchase requisitions, automatically notifying the appropriate user of the need to authorise a requisition electronically).</td>
</tr>
</tbody>
</table>
Appendix 2: Upgrading to ECC

This Appendix provides an overview of key security and control functionality that should be considered when performing an upgrade from SAP R/3 to ECC 5.0 or ECC 6.0.

When upgrading SAP, an entity makes the decision to either perform a technical upgrade or a functional upgrade. A technical upgrade involves only upgrading the technology underlying the SAP system.

When upgrading to ECC, most entities typically choose to perform a technical upgrade.

The standard technical upgrade can usually be performed by the Basis administrators without issue. A functional upgrade which enables new functionality to be configured requires a more robust project approach.

Challenges experienced in functional upgrade projects include:

- Time and cost estimations and overruns;
- Justification of the project budget;
- Managing the project;
- Assessing the impact on existing computing and business solutions;
- Identifying business requirements;
- An effective and efficient level of quality testing; and
- Minimising system downtime.

In addition to project risk factors, there are several security and control configuration considerations when upgrading to ECC 5.0 or ECC 6.0.

1. New General Ledger
2. PRG_CUST Security Parameter
3. System security (RSPARAM settings)
1. Implementation of the New General Ledger

Within ECC, a New General Ledger component has been introduced. Entities can choose to either use the traditional General Ledger component or to implement the New General Ledger. Earlier Chapters highlight implementation considerations and risks.

Chapter 3: General Ledger, Risk 310

2. PRG_CUST Security Parameter – New IMG setting.

This is a new system security parameter that has been introduced in ECC. The parameter allows access to assign roles and maintain roles to be segregated.

The ASSIGN_ROLE_AUTH should be set to value ASSIGN so that the authorisation values required for assigning roles to users do not also grant the ability to modify the authorisations of the role.

Chapter 5: Basis, Optimising the SAP Control Environment (Security controls)

3. New System Security Parameters

ECC 5.0 and 6.0 provides a number of new system parameters which may be implemented to improve system security:

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Description / Importance of Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>login/min_password_diff</td>
<td>This parameter defines how many characters in the new password must differ from the old password.</td>
</tr>
<tr>
<td>login/min_password_digits</td>
<td>This parameter specifies the minimum number of digits that a user’s password must contain.</td>
</tr>
<tr>
<td>login/min_password_letters</td>
<td>This parameter specifies the minimum number of letters that a user’s password must contain.</td>
</tr>
<tr>
<td>login/min_password_specials</td>
<td>This parameter specifies the minimum number of special characters that a user’s password must contain.</td>
</tr>
<tr>
<td>login/password_max_new_valid</td>
<td>Defines the number of days before an initial password set up for a new user expires.</td>
</tr>
<tr>
<td>login/password_max_reset_valid</td>
<td>Defines the number of days before a reset user password expires.</td>
</tr>
</tbody>
</table>

Chapter 5: Basis, Risk 505

Entities should ensure that configuration settings comply with their Agency Security Policy. For further detail, the Australian Government Information and Communications Technology Security Manual (ISM) contains further detail on appropriate logical access controls. Refer to (www.dsd.gov.au) for further detail.
Appendix 3: SAP and segregation of duties risks

Segregation of duties (SoD) is a primary internal control used when undertaking financial operations, which is intended to prevent a single individual from having control over all stages of financial transactions. The objective of segregation of duties is to ensure that different people are involved in the different stages of a transaction, consisting mainly of the initiation, authorisation/approval, recording, and settlement processes.

Common SAP access exposures

A SoD conflict can occur within a role (inherent role conflicts) or through the allocation of multiple roles to the one user. In the context of SAP security, there are two types of common access exposures:

- **SAP Role Conflict**
  Conflicts that arise from a security object (profile/role/class/etc.) being defined with excessive (Critical access) or conflicting privileges within one role.

- **User Role Allocation Conflict**
  Conflicts that arise from multiple security profiles/roles/classes being assigned to a user account such that the cumulative privileges of the user are excessive or conflicting (between roles).

The following list provides examples of undesirable actions that could be performed if particular functions are not restricted:

- Ability to create a ghost vendor and process a payment to that vendor.
- Ability to change a vendor bank account and process a payment to a fraudulent bank account.
- Ability to purchase an attractive asset and misappropriate it.
- Ability to process a purchase order to a ghost vendor.
Implementing segregation of duties in SAP

The following table outlines factors that should be considered when implementing a segregation of duties ruleset:

<table>
<thead>
<tr>
<th>Ruleset</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User access risk</td>
<td>A risk is an opportunity for physical loss, fraud, process disruption, or productivity loss that occurs when user access exploit a specific condition. Identify conflicting or incompatible functions. An example of a segregation of duties risk is Vendor Maintenance versus Invoice Entry. These functions should be segregated to restrict the ability of a user to create a ghost vendor and process an unauthorised payment to the vendor.</td>
</tr>
<tr>
<td>Function</td>
<td>A function is a grouping of one or more relate actions and/or permissions for a specific business area, such as Asset management. It is also referred to as a ‘transaction group’. An example of a function is Vendor Maintenance. This function would include all of the SAP transactions that can be used to maintain a vendor account.</td>
</tr>
<tr>
<td>Transaction</td>
<td>A transaction that can be used in SAP to fulfil a specific Function (e.g. ME21 Create Purchase Order, Create FK01 Vendor Master Record).</td>
</tr>
<tr>
<td>Authorisation Object and Field Values</td>
<td>Authorisation objects allow users to perform a particular activity in a system. An example of an authorisation object and field for the Vendor Maintenance function would be authorisation object F_LFA1_BUK which restricts users’ ability to create or change vendor accounts by company code.</td>
</tr>
<tr>
<td>Conflicting Transactions</td>
<td>Individual transaction combinations that are reviewed to identify segregation of duties conflicts. This assists in identifying SAP roles</td>
</tr>
</tbody>
</table>

Links to other chapters in this guide

The following are links to case studies and examples referenced throughout the guide:

- Chapter 2: Procurement and Payables – Eliminating vendor maintenance segregation of duty risks
- Chapter 4: Human Resources – Periodic assessment of employees paid as vendors
- Feature article 5: GRC Access control – Implementing preventative segregation of duties checking
- Feature article 5: GRC Access control – User vs role based security
## User access risks

The following table recommends, using a generic business process description, those functions that should be segregated. The table does not include processes related to system maintenance (ie Basis).

<table>
<thead>
<tr>
<th>Process</th>
<th>Function 1</th>
<th>Function 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement / Purchasing</td>
<td>Purchasing Document Creator</td>
<td>Purchasing Document Approver</td>
</tr>
<tr>
<td></td>
<td>Purchasing Approver</td>
<td>Goods Receipt</td>
</tr>
<tr>
<td>Supplier Relationship Management (SRM)</td>
<td>SRM – Create or maintain shopping cart</td>
<td>SRM – Approve shopping cart</td>
</tr>
<tr>
<td></td>
<td>ERP – Vendor Maintenance</td>
<td>SRM – Create or maintain shopping cart</td>
</tr>
<tr>
<td></td>
<td>ERP – Vendor Maintenance</td>
<td>SRM – Approve shopping cart Purchase Orders</td>
</tr>
<tr>
<td></td>
<td>ERP – Invoice Entry</td>
<td>SRM – Create or maintain shopping cart</td>
</tr>
<tr>
<td></td>
<td>ERP – Invoice Entry</td>
<td>SRM – Approve shopping cart Purchase Orders</td>
</tr>
<tr>
<td></td>
<td>ERP – Goods Receipt</td>
<td>SRM – Create or maintain shopping cart</td>
</tr>
<tr>
<td></td>
<td>ERP – Goods Receipt</td>
<td>SRM – Approve shopping cart Purchase Orders</td>
</tr>
<tr>
<td>Vendor Master File</td>
<td>Vendor Maintenance</td>
<td>Bank Reconciliation</td>
</tr>
<tr>
<td></td>
<td>Vendor Maintenance</td>
<td>Purchase Orders</td>
</tr>
<tr>
<td></td>
<td>Vendor Maintenance</td>
<td>Vendor Invoice / Payments</td>
</tr>
<tr>
<td>Goods Receipt</td>
<td>Goods Receipt</td>
<td>AP Invoice Entry</td>
</tr>
<tr>
<td></td>
<td>Goods Receipt</td>
<td>Purchase Document Entry or Approval</td>
</tr>
<tr>
<td></td>
<td>Goods Receipt</td>
<td>Asset Master Maintenance</td>
</tr>
<tr>
<td></td>
<td>Goods Receipt</td>
<td>Material Master Maintenance</td>
</tr>
<tr>
<td></td>
<td>Goods Receipt</td>
<td>Vendor Maintenance</td>
</tr>
<tr>
<td></td>
<td>Services Master Maintenance</td>
<td>Service Acceptance</td>
</tr>
<tr>
<td>Invoice Processing</td>
<td>Invoice Entry</td>
<td>Invoice Release</td>
</tr>
<tr>
<td></td>
<td>Invoice Entry</td>
<td>Vendor Payments</td>
</tr>
<tr>
<td></td>
<td>Invoice Entry</td>
<td>Purchase Document Approvals</td>
</tr>
<tr>
<td></td>
<td>Invoice Entry</td>
<td>Vendor Maintenance</td>
</tr>
<tr>
<td>Payment Processing</td>
<td>Vendor Payments / Manual Payments</td>
<td>Purchase Document Approval</td>
</tr>
<tr>
<td></td>
<td>Vendor Payments / Manual Payments</td>
<td>Vendor Maintenance</td>
</tr>
<tr>
<td></td>
<td>Vendor Payments / Manual Payments</td>
<td>Bank Maintenance</td>
</tr>
<tr>
<td>Process</td>
<td>Function 1</td>
<td>Function 2</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>General Ledger Master Maintenance, Postings</td>
<td>General Ledger account maintenance</td>
<td>Journal Processing</td>
</tr>
<tr>
<td>and Reconciliation</td>
<td>Maintain Posting Periods</td>
<td>Journal Processing</td>
</tr>
<tr>
<td></td>
<td>General Ledger account maintenance</td>
<td>Foreign Currency</td>
</tr>
<tr>
<td>HR Personnel Management</td>
<td>Employee Maintenance</td>
<td>Payroll Processing</td>
</tr>
<tr>
<td></td>
<td>Employee Maintenance</td>
<td>Position Management</td>
</tr>
<tr>
<td></td>
<td>Employee Maintenance – Bank Account</td>
<td>Employee Maintenance – Payroll Status</td>
</tr>
<tr>
<td>Personal Time Management</td>
<td>Timesheet Entry</td>
<td>Timesheet Approval</td>
</tr>
<tr>
<td></td>
<td>Timesheet Assessment</td>
<td>Process Payroll</td>
</tr>
<tr>
<td>Payroll Accounting</td>
<td>Payroll Processing</td>
<td>Employee Maintenance</td>
</tr>
<tr>
<td></td>
<td>Payroll Processing</td>
<td>Payroll Configuration</td>
</tr>
<tr>
<td></td>
<td>Payroll Processing</td>
<td>Position Management</td>
</tr>
<tr>
<td>Controlling</td>
<td>Cost Structure Maintenance</td>
<td>Cost Centre Transfer</td>
</tr>
<tr>
<td></td>
<td>Cost Structure Maintenance</td>
<td>AP Invoice Entry</td>
</tr>
<tr>
<td></td>
<td>Cost Structure Maintenance</td>
<td>Purchase Orders</td>
</tr>
<tr>
<td></td>
<td>Internal Order Maintenance</td>
<td>Settle Internal Order Costs</td>
</tr>
<tr>
<td>Project System</td>
<td>Define WBS Elements</td>
<td>Project Settlement</td>
</tr>
<tr>
<td></td>
<td>Define WBS Elements</td>
<td>Overhead Posting</td>
</tr>
<tr>
<td></td>
<td>Project Settlement</td>
<td>Asset Master Record Maintenance</td>
</tr>
<tr>
<td></td>
<td>Project Settlement</td>
<td>Overhead Posting</td>
</tr>
<tr>
<td>Asset Master Maintenance</td>
<td>Asset Master Record Maintenance</td>
<td>Asset Transactions</td>
</tr>
<tr>
<td></td>
<td>Accounts Payable Invoices</td>
<td>Asset Master Record Maintenance</td>
</tr>
<tr>
<td></td>
<td>Purchase Order Processing</td>
<td>Asset Master Record Maintenance</td>
</tr>
<tr>
<td>Asset Transaction Postings</td>
<td>Asset Master Record Maintenance</td>
<td>Asset Transactions</td>
</tr>
<tr>
<td>Grants Management</td>
<td>Approve Grant</td>
<td>Record Grant</td>
</tr>
<tr>
<td></td>
<td>Maintain Grant Cost</td>
<td>Settle Project Costs</td>
</tr>
</tbody>
</table>
**Index**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset Accounting</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>229</td>
</tr>
<tr>
<td>Asset Master Maintenance</td>
<td>230</td>
</tr>
<tr>
<td>Asset Transaction Postings</td>
<td>235</td>
</tr>
<tr>
<td><strong>Basis</strong></td>
<td></td>
</tr>
<tr>
<td>Transport Management System</td>
<td>120</td>
</tr>
<tr>
<td>Security</td>
<td>127</td>
</tr>
<tr>
<td>Table and Program Maintenance</td>
<td>146</td>
</tr>
<tr>
<td>Basis System Administration</td>
<td>152</td>
</tr>
<tr>
<td>Mass Maintenance</td>
<td>160</td>
</tr>
<tr>
<td>NetWeaver Security</td>
<td>164</td>
</tr>
<tr>
<td>Central User Administration</td>
<td>167</td>
</tr>
<tr>
<td>Backup and Recovery</td>
<td>169</td>
</tr>
<tr>
<td>Portal Security (SAP Enterprise Portal)</td>
<td>171</td>
</tr>
<tr>
<td><strong>Commonly identified control weaknesses</strong></td>
<td></td>
</tr>
<tr>
<td>Asset Accounting</td>
<td></td>
</tr>
<tr>
<td>Asset Master Maintenance</td>
<td>231</td>
</tr>
<tr>
<td>Asset Transaction Postings</td>
<td>236</td>
</tr>
<tr>
<td>Basis</td>
<td></td>
</tr>
<tr>
<td>Transport Management System</td>
<td>120</td>
</tr>
<tr>
<td>Security</td>
<td>128</td>
</tr>
<tr>
<td>Table &amp; Program Maintenance</td>
<td>146</td>
</tr>
<tr>
<td>Basis System Admin.</td>
<td>152</td>
</tr>
<tr>
<td>Mass Maintenance</td>
<td>160</td>
</tr>
<tr>
<td>Controlling</td>
<td>201</td>
</tr>
<tr>
<td><strong>General Ledger</strong></td>
<td></td>
</tr>
<tr>
<td>General Ledger Master Maintenance</td>
<td>65</td>
</tr>
<tr>
<td>General Ledger Postings / Reconciliation</td>
<td>71</td>
</tr>
<tr>
<td>New General Ledger</td>
<td>79</td>
</tr>
<tr>
<td><strong>GRC Access Control</strong></td>
<td></td>
</tr>
<tr>
<td>Risk Analysis &amp; Remediation</td>
<td>178</td>
</tr>
<tr>
<td>Superuser Privilege Mgmt (Firefighter)</td>
<td>188</td>
</tr>
<tr>
<td><strong>Human Resources</strong></td>
<td></td>
</tr>
<tr>
<td>Personnel Management</td>
<td>90</td>
</tr>
<tr>
<td>Personal Time Mgmt</td>
<td>98</td>
</tr>
<tr>
<td>Payroll Accounting</td>
<td>103</td>
</tr>
<tr>
<td>Employee Self Service</td>
<td>110</td>
</tr>
<tr>
<td>Managers Desktop</td>
<td>114</td>
</tr>
<tr>
<td><strong>Project System</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Purchasing and payables</strong></td>
<td></td>
</tr>
<tr>
<td>Procurement and purchasing activities</td>
<td>14</td>
</tr>
<tr>
<td>Supplier Relationship Management</td>
<td>23</td>
</tr>
<tr>
<td>Vendor Master File</td>
<td>29</td>
</tr>
<tr>
<td>Material Master File</td>
<td>36</td>
</tr>
<tr>
<td>Receipt of goods or services</td>
<td>40</td>
</tr>
<tr>
<td>Invoice Processing</td>
<td>47</td>
</tr>
<tr>
<td>Payment Processing</td>
<td>44</td>
</tr>
<tr>
<td><strong>Controlling</strong></td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>199</td>
</tr>
<tr>
<td>Functional overview</td>
<td>200</td>
</tr>
<tr>
<td>Commonly identified control weaknesses</td>
<td>201</td>
</tr>
<tr>
<td>Significant Risks</td>
<td>201</td>
</tr>
<tr>
<td>Risks and controls</td>
<td>202</td>
</tr>
<tr>
<td>Security considerations</td>
<td>205</td>
</tr>
<tr>
<td>Optimising the SAP control environment</td>
<td>207</td>
</tr>
<tr>
<td><strong>Feature articles</strong></td>
<td></td>
</tr>
<tr>
<td>Shared services</td>
<td>81</td>
</tr>
<tr>
<td>GRC Access Control</td>
<td>173</td>
</tr>
<tr>
<td>Grants management</td>
<td>221</td>
</tr>
<tr>
<td><strong>General Ledger</strong></td>
<td></td>
</tr>
<tr>
<td>General Ledger Master Maintenance</td>
<td>64</td>
</tr>
<tr>
<td>General Ledger Postings / Reconciliation</td>
<td>71</td>
</tr>
<tr>
<td>New General Ledger</td>
<td>78</td>
</tr>
<tr>
<td><strong>Human Resources</strong></td>
<td></td>
</tr>
<tr>
<td>Personnel Management</td>
<td>90</td>
</tr>
<tr>
<td>Personal Time Mgmt</td>
<td>98</td>
</tr>
<tr>
<td>Payroll Accounting</td>
<td>102</td>
</tr>
<tr>
<td>Employee Self Service</td>
<td>110</td>
</tr>
<tr>
<td>Managers Desktop</td>
<td>114</td>
</tr>
<tr>
<td><strong>Implementation considerations</strong></td>
<td></td>
</tr>
<tr>
<td>Shared Services</td>
<td>86</td>
</tr>
<tr>
<td><strong>Introduction</strong></td>
<td></td>
</tr>
<tr>
<td>Purpose of this guide</td>
<td>3</td>
</tr>
<tr>
<td>Structure</td>
<td>3</td>
</tr>
<tr>
<td>Why consider controls?</td>
<td>4</td>
</tr>
<tr>
<td>Previous guides and this guide</td>
<td>4</td>
</tr>
<tr>
<td>How to read this guide</td>
<td>5</td>
</tr>
<tr>
<td><strong>Procurement and payables</strong></td>
<td></td>
</tr>
<tr>
<td>Procurement and purchasing activities</td>
<td>9</td>
</tr>
<tr>
<td>Supplier Relationship Management (SRM)</td>
<td>22</td>
</tr>
<tr>
<td>Vendor Master File</td>
<td>29</td>
</tr>
</tbody>
</table>
### IMPORTANT UPDATE

<table>
<thead>
<tr>
<th>Material Master File</th>
<th>36</th>
<th>Security considerations</th>
<th>217</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receipt of goods or services</td>
<td>40</td>
<td>Optimising the SAP control environment</td>
<td>218</td>
</tr>
<tr>
<td>Invoice processing</td>
<td>46</td>
<td>SAP and segregation of duties risks</td>
<td>267</td>
</tr>
<tr>
<td>Payment processing</td>
<td>55</td>
<td>Security considerations</td>
<td>-</td>
</tr>
</tbody>
</table>

### Optimising SAP controls

**Asset Accounting**
- Asset Master Maintenance: 234
- Asset Transaction Postings: 243

**Basis**
- Transport Mgmt Syst.: 126
- Security: 143-144
- Table & Program Maintenance: 151
- Basis System Admin.: 159
- Mass Maintenance: 163
- Risk Analysis & Remediation: 184-185
- Superuser Privilege Mgmt (Firefighter): 195

**Controlling**
- 207

**General Ledger**
- General Ledger master maintenance: 70
- General Ledger Postings / Reconciliation: 77
- New General Ledger: 80

**Human Resources**
- Personnel Management: 96
- Personal Time Mgmt: 101
- Payroll Accounting: 108
- Employee Self Service: 113
- Managers Desktop: 116

**Project System**
- 218-219

**Purchasing and payables**
- Procurement and purchasing activities: 20
- Supplier Relationship Management: 28
- Vendor Master File: 35
- Material Master File: 39
- Receipt of goods or services: 44
- Invoice processing: 54
- Payment processing: 59

**Project System**
- 209

**GRC Access Control**
- 205-206

**Controlling**
- Project System: 217-218

**Grants management**
- 225

**Asset Accounting**
- 233-234

**Terminology and Definitions**
- 247

**Upgrading to ECC**
- 265
## Index of Case studies

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Sub-process</th>
<th>Case study title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement and payables</td>
<td>Procurement and purchasing activities</td>
<td>Setting up release strategy approval limits</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Vendor master file</td>
<td>Eliminating vendor maintenance segregation of duties</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td></td>
<td>concerns using dual control for sensitive fields</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vendor master file</td>
<td>One-time vendor (OTV) payments</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Invoice Processing</td>
<td>Duplicate invoice check</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OCR invoice scanning</td>
<td>53</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Personnel Management</td>
<td>Periodic assessment for employees who are paid as vendors</td>
<td>92</td>
</tr>
<tr>
<td>Basis</td>
<td>Security</td>
<td>Cross-Talk in SAP Security</td>
<td>129</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitoring for Cross-Talk issues which result in problems with access across organisational areas</td>
<td>130</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td>Single sign-on for SAP systems</td>
<td>135</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td>User versus position based security</td>
<td>145</td>
</tr>
<tr>
<td></td>
<td>Table and Program Maintenance</td>
<td>Logging changes to critical tables</td>
<td>148</td>
</tr>
<tr>
<td>GRC Access Control</td>
<td>Risk Analysis and Remediation</td>
<td>Implementing preventative controls to monitor segregation of duties risk</td>
<td>183</td>
</tr>
<tr>
<td>Asset Management</td>
<td>Asset Transaction Postings</td>
<td>Improving the accuracy of depreciation charges using Asset Class Useful Life configuration controls</td>
<td>239</td>
</tr>
</tbody>
</table>

## Index of Significant risks

### Purchasing and payables
- **H R200**: Unapproved purchase requisitions/orders are created 15
- **H R201**: Changes are made to approved requisitions or orders 16
- **H R202**: Purchase orders do not reference purchase requisitions 16
- **M R203**: Approved blanket purchase order values are exceeded 17
- **M R204**: Non-strategic vendors are used for purchasing 17
- **M R205**: Invoice and goods receipt settings are changed in purchase order creation 18

### Supplier Relationship Management
- **H R206**: Unauthorised purchases are made by SRM users 24
- **H R207**: Changes are made to orders after approvals have been gained 25
- **H R208**: Inappropriate invoices are entered into the system 25

### Vendor master file
- **H R209**: Unapproved or incorrect changes are made to vendor records 30
- **H R210**: Inappropriate use of the alternative payee function 31
- **H R211**: Vendor records are not allocated to a reconciliation account 32
- **M R212**: Duplicate vendor records are created 32
- **M R213**: Incorrect payments are made through one-time vendor account 33

### Material master file
- **H R214**: Material master integrity concerns including valuation issues 37
- **H R215**: Inventory balances recorded in the material master do not exist 37
- **M R216**: Duplicate material items exist 38

### Receipt of goods or services
- **H R217**: Unapproved or incorrect purchase requisitions are created 41
- **H R218**: Goods receipt quantity differs from ordered quantity 42
- **M R219**: Damaged goods are accepted 42
<table>
<thead>
<tr>
<th>Process</th>
<th>Type</th>
<th>Issue Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoice processing</td>
<td>H</td>
<td>R220: Duplicate invoices are processed</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>R221: Unapproved or incorrect non-order invoices are created</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>R222: Incorrect purchase order payments are processed</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>R223: Goods Receipt (GR) / Invoice Receipt (IR) account is not adequately reconciled</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R224: Parked and blocked invoices are not actioned</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R225: Returned goods are still invoiced</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R226: Inappropriate changes are made to invoices after processing</td>
<td>52</td>
</tr>
<tr>
<td>Payment processing</td>
<td>H</td>
<td>R227: Unauthorised or incorrect EFT payments are processed</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>R228: Inappropriate changes are made to payments in the payment program</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>R229: Unapproved or incorrect manual payments are made</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R230: Incorrect changes made to recurring payments</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R231: Payment methods are not assigned to vendor accounts</td>
<td>58</td>
</tr>
<tr>
<td>General Ledger</td>
<td>H</td>
<td>R300: General Ledger system is inadequately configured</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>R301: Duplicate, incorrect, or unauthorised maintenance of General Ledger accounts</td>
<td>67</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R302: Incorrect maintenance of accounting periods</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R303: Incorrect maintenance of exchange rates</td>
<td>68</td>
</tr>
<tr>
<td>General Ledger Postings /</td>
<td>H</td>
<td>R304: Ineffective reconciliation of SAP modules and external interfaces</td>
<td>72</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>H</td>
<td>R305: Duplicate or incorrect General Ledger journals</td>
<td>73-74</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>R306: Failure to adequately reconcile key bank accounts</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R307: Negative postings are permitted</td>
<td>74</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R308: Parked journals are not actioned on a timely basis</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R309: Failure to adequately perform period end procedures</td>
<td>75</td>
</tr>
<tr>
<td>New General Ledger</td>
<td>H</td>
<td>R310: New General Ledger is inadequately configured</td>
<td>79</td>
</tr>
<tr>
<td>Human Resources</td>
<td>H</td>
<td>R400: Employee master integrity concerns / employee cost allocations are incorrect</td>
<td>91</td>
</tr>
<tr>
<td>Personnel Management</td>
<td>H</td>
<td>R401: Employees are not inactivated when employment is terminated</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>R402: Unauthorised changes to employee positions and appointments</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>R403: Users are able to view sensitive employee data</td>
<td>93</td>
</tr>
<tr>
<td>Payroll accounting</td>
<td>M</td>
<td>R404: Inaccurate or untimely entry of timesheet data</td>
<td>99</td>
</tr>
<tr>
<td>Employee Self Service</td>
<td>M</td>
<td>R412: Excessive or unauthorised access to sensitive HR data</td>
<td>111</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R413: Leave taken is not accurately recorded</td>
<td>112</td>
</tr>
<tr>
<td>Managers Desktop</td>
<td>H</td>
<td>R414: Unauthorised approval of time, expense or other employee or HR data</td>
<td>115</td>
</tr>
<tr>
<td>Basis</td>
<td>H</td>
<td>R500: Emergency changes are not managed appropriately</td>
<td>121-123</td>
</tr>
<tr>
<td></td>
<td>H</td>
<td>R501: Emergency changes are not managed appropriately</td>
<td>123</td>
</tr>
<tr>
<td></td>
<td>M</td>
<td>R502: Access to test and quality systems is not appropriately restricted</td>
<td>124</td>
</tr>
</tbody>
</table>
Security
H R503: Incorrect implementation of administration/ownership policy 131-132
H R504: Inappropriate security administration processes 132
H R505: Ineffective established security parameters 133-134
H R506: Inappropriate access to key SAP privileges 136
H R507: Access is allocated to incompatible transactions 137
M R508: Unauthorised OSS access 137
M R509: Inappropriate access to SAP utilities 138
M R510: Inappropriate derived role maintenance and configuration 138
M R511: Insufficient reporting security 139
M R512: Use of standard SAP roles or profiles 140
M R513: Inappropriate operating system access 140
M R514: Unauthorised database access is obtained 140

Table & Program Maint.
H R515: Changes to critical database tables are not logged 147
H R516: Users have the ability to modify programs in production 148
H R517: Inappropriate access to the data dictionary 148
M R518: Tables and programs are not restricted by authorisation group 148

Basis System Admin.
H R519: SAP security authorisation checks are turned off 153
H R520: SAP database is not properly maintained 154
M R521: Inadequate user and system documentation 155
M R522: Client, country and company code configuration is inadequate 156
M R523: SAProuter settings are incorrect 156

Mass maint.
H R524: Inappropriate or unauthorised changes made to data 161

Central User Admin.
M R525: CUA configuration and ALE landscape may not be configured correctly 167

Backup and Recovery
H R526: Critical SAP data is lost 170

GRC Access Control
Risk Analysis & Remediation
H R550: Inadequate configuration of segregation of duties ruleset 179
H R551: Ineffective identification, documentation or over-reliance on mitigation controls 180
H R552: Failure to implement preventative segregation of duties checking 181
M R553: Incorrect setup of overall configuration options 181-182

Superuser Privilege Mgmt (Firefighter)
H R554: Inadequate Firefighter configuration 189-191
H R555: Failure to effectively review Firefighter activity logs 192
M R556: Using Firefighter to remediate segregation of duties issues rather than for support purposes. 193
M R557: Definition of an incorrect set of critical transactions 194

Controlling
H R600: Reconciliation problems between the FI and CO modules 202
H R601: Ineffective maintenance of Controlling Master Data 203
H R602: Incorrect allocations or reversal of costs to Cost Centres 204
H R603: Incorrect or failure to settle internal order costs 204

Project System
H R700: Incorrect set up or changes to the Work Breakdown Structure 213
H R701: Configuration issues with Settlement rules 214
H R702: Inadequate project justification or unapproved projects 214
H R703: Inadequate management of project timeframes, deliverables and costs 215
M R704: Projects are not closed or are closed with open commitments 216
M R705: Project system does not interface to the General Ledger 216
<table>
<thead>
<tr>
<th>Grants management</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Grants management</td>
<td>H</td>
</tr>
<tr>
<td>H R710: Inappropriate establishment approval of each Grant project</td>
<td>224</td>
</tr>
<tr>
<td>H R711: Untimely settlement of costs</td>
<td>224</td>
</tr>
<tr>
<td>H R712: Allocation of costs against the incorrect project</td>
<td>225</td>
</tr>
<tr>
<td>Asset Accounting</td>
<td></td>
</tr>
<tr>
<td>Asset Master Maintenance</td>
<td>H</td>
</tr>
<tr>
<td>H R800: High value assets are entered into a low value asset class</td>
<td>231</td>
</tr>
<tr>
<td>M R801: Duplicate or incomplete Asset Master Records are created</td>
<td>232</td>
</tr>
<tr>
<td>M R802: Asset records on the Asset Register do not exist</td>
<td>233</td>
</tr>
<tr>
<td>Asset Transaction Postings</td>
<td>H</td>
</tr>
<tr>
<td>H R803: Asset depreciation charges are incorrect</td>
<td>237-238</td>
</tr>
<tr>
<td>H R804: Expenditure is not correctly capitalised</td>
<td>239</td>
</tr>
<tr>
<td>H R805: Acquisitions are not approved</td>
<td>240</td>
</tr>
<tr>
<td>H R806: Failure to record all Asset transactions within the General Ledger</td>
<td>240</td>
</tr>
<tr>
<td>M R807: Asset retirements and transfers are processed incorrectly</td>
<td>241</td>
</tr>
<tr>
<td>M R808: Asset Revaluations are incorrectly performed</td>
<td>242</td>
</tr>
</tbody>
</table>
SAP ECC 6.0: Security and control

The ANAO proposes to update this Guide in 2015-2016 to reflect upgrades to SAP since 2009 and the growing use of SAP across Australian Government entities.