Security and Control
For SAP R/3

Guide to Effective Control
Acknowledgements

Thanks are extended to the following agencies who allowed the ANAO to review their SAP R/3 sites for the purpose of developing the handbook:

- Department of Communications and the Arts;
- Health Services Australia; and
- Department of Workplace Relations and Small Business (limited pre-implementation review).

Appreciation is also extended to PricewaterhouseCoopers who contributed significantly in developing and writing this handbook and who also provided expert SAP advice and assistance in the review of the various SAP R/3 sites.

Disclaimer

This handbook is not a recommendation of the SAP R/3 system, nor an endorsement of the SAP R/3, by the ANAO. Commonwealth Public Sector agencies are responsible for deciding whether SAP R/3 is suitable for their purposes and for implementing and testing SAP R/3.

The Auditor-General, the ANAO, its officers and employees are not liable, without limitation, for any consequences incurred, or any loss or damage suffered by an agency or by any other person as a result of their reliance on the information contained in this handbook or resulting from their implementation or use of the SAP R/3 system, and to the maximum extent permitted by law, exclude all liability (including in negligence) in respect of the handbook or its use.
Preface

The current exposure draft on Information Security which will form part of the new Protective Security Manual released by the Protective Security Coordination Centre mentions that the primary responsibility for ensuring the availability and integrity of official information rests with Commonwealth Public Sector agencies. Any information developed, received or collected, by or on behalf of the Government, is regarded as official information and must be handled with care and only in accordance with authorised procedures.

In addition, each individual IT system will require a risk assessment and system security plan, which must be consistent with and complement the overall agency IT security plan.\footnote{See exposure draft on ‘Guidelines for Managing Security Risk - Commonwealth Protective Security Manual Volume B’ for further information on security plans.}

SAP being a financial and human resource management information system also contains official information. Therefore agencies will have a responsibility to ensure that the availability, integrity and confidentiality of the information within SAP is well controlled.

This handbook will assist agencies in meeting this obligation by outlining the security and internal control mechanisms in the form of best practice procedures that can be used by an agency to protect and control the financial information within the SAP system. This handbook highlights three types of best practice procedures. These are:

- best practice procedures considered critical to achieving an acceptable level of control, which if not implemented will result in significant risks to the organisation;
- best practice procedures which are considered important to achieving a good level of internal control but which if not implemented would not result in a high risk to the organisation; and
- best practice procedures which do not have a significant impact on the overall control environment but which may assist the control or efficiency of the business process.

The adoption of these procedures will depend on how SAP R/3 is used within each agency and the level of acceptable risk adopted by that agency. As mentioned in our better practice guide on effective control, striving for absolute assurance is neither cost effective nor possible. Controls implemented should be commensurate with the nature of the business, the acceptable level of risk and program delivery.
## Contents

**Introduction**
- SAP R/3 - What is it? .............................................................. 1
- Why was the handbook developed? ........................................ 1
- What modules are covered in the handbook? .......................... 2
- How can this handbook help me? ............................................ 3
- Critical areas not covered by this handbook ............................ 3
- Applicability of the handbook to ANAO financial statement audits 4
- Why is SAP security and control different? ............................ 4
- How to read the better practice handbook .............................. 6
- Introduction to SAP concepts .................................................. 7

**Procurement to payables** .................................................. 9
- Section contents ........................................................................ 9
- Procurement cycle overview .................................................. 11
- Procurement/purchasing activities ......................................... 13
- Vendor master file ..................................................................... 20
- Material master file .................................................................... 26
- Receipt of goods/services ...................................................... 30
- Invoice verification (Materials management) .......................... 39
- Accounts payable (Financial accounting) ............................... 50
- Payment processing .............................................................. 61

**Financial accounting** ....................................................... 69
- Section contents ........................................................................ 69
- General ledger master maintenance ...................................... 72
- Customer master maintenance .............................................. 76
- General ledger processing .................................................... 82
- Asset accounting ...................................................................... 92
- Asset overview ......................................................................... 92
- Asset acquisition process ..................................................... 93
- Asset transfer/retirement process ......................................... 98
- Asset depreciation/periodic processing ................................ 102
Controlling
Section contents ..................................................................................................................................................107
Cost allocations and transaction postings ........................................................................................................109

Human resources
Section contents ..................................................................................................................................................115
Personnel/human resources functions ........................................................................................................117
Payroll calculation and payment ..................................................................................................................125

Basis component and cross-application matters
Section contents ..................................................................................................................................................137
Environment ................................................................................................................................................140
Security .......................................................................................................................................................149
Change control ..............................................................................................................................................163
Interfaces with external systems ................................................................................................................169
Data conversion ............................................................................................................................................176

Appendix I: Introduction to SAP concepts
Section contents ..................................................................................................................................................181
Organisational structures in SAP ................................................................................................................182
The implementation guide ..........................................................................................................................184
Numbering in SAP ....................................................................................................................................185
Sub-ledger reconciliations ..........................................................................................................................185
Document types and postings keys .............................................................................................................185
Validations and substitutions ......................................................................................................................185
Field status ................................................................................................................................................186
Document changes rules ............................................................................................................................187
Reporting and report trees ........................................................................................................................187
Audit trails and logging ................................................................................................................................189
Introduction to SAP security concepts ......................................................................................................189

Appendix 2: Glossary of terms .....................................................................................................................193

Index .............................................................................................................................................................205
Introduction

SAP R/3 - What is it?

SAP R/3 is a large integrated data processing system. SAP provides the complex application software required to support the various business processes of the organisation including:

- Financial accounting.
- Logistics/supply.
- Sales and distribution.
- Human resources.

SAP R/3’s main strength is its integrated and modular architecture. Organisations may choose to implement all or only a few of the many application modules which are totally integrated within the system on a real-time basis. Introduced in 1992, SAP R/3 is a client/server based enterprise wide business solution and is currently one of the largest selling business software packages.

Why was the handbook developed?

SAP R/3 has been implemented in a number of significant Commonwealth agencies. It is a very complex product and requires considerable investment by agencies in its implementation. As many modules and functions within SAP are fully integrated, agencies must make a substantial commitment of time and resources to re-engineer their business processes to ensure consistency within SAP. If agencies do not implement SAP correctly, then considerable resources will be required to correct any later identified problems. This could not only be costly, but may also be embarrassing to the agency concerned and consequently the government.

This handbook is intended to assist Commonwealth Public Sector agencies in ensuring that security considerations and internal controls in the form of ‘better practice procedures’ within the SAP system are configured or developed correctly. The handbook will be most useful to those agencies who are intending to implement SAP. It would also be useful for agencies who have already implemented SAP but need to revisit their security and internal control configuration. However, it does not purport to contain all the information necessary to assess whether to implement SAP and should not be used as a substitute for a proper decision making process concerning the system’s implementation.

SAP Australia is currently developing a public sector template which consists of a pre-defined SAP configuration plus some additional functionality that will be useful for public sector agencies. It should be noted that the security and internal control mechanisms mentioned in this handbook may not necessarily be addressed by the adoption of this template.
What modules are covered in the handbook?

This handbook covers those modules of SAP R/3 that are most likely to be implemented by Commonwealth agencies. These being:

- Basis component (BC).
- Materials management (MM); in this handbook refer to ‘Procurement to payables’.
- Financial accounting (FI).
- Controlling (CO).
- Asset accounting (FI-AA); incorporated in the financial accounting module of this handbook.
- Human resources (HR).

The better practice procedures and standard features identified in this handbook are based on SAP R/3 release 3.1H. Although most also apply to earlier releases of SAP, a small number of the features described may not be applicable in those earlier releases.

The ANAO intends to provide, where applicable, updates to the handbook on an annual basis to reflect any additional features included in new releases of SAP. Updates will be provided electronically via the ANAO’s Internet address: http://www.anao.gov.au.
How can this handbook help me?

The handbook highlights those 'best practice procedures' which, if not implemented by the agency, will result in various risks to the organisation. Ideally, implementation of all the 'best practice procedures' would be desirable. However, organisations do vary in size and resources so that the adoption of 'best practice procedures' identified for each risk will depend on how SAP is used within each agency and the level of acceptable risk adopted by that agency based on their risk management strategy. These 'best practice procedures' are control activities that ensure:

• There is mitigation of risks.
• Irregularities are prevented or detected and corrected.
• Financial assets are safeguarded from unauthorised use or disposal.
• Financial records and other relevant databases are complete, accurately reflect the entire operational activities of the agency and assist in the timely preparation of accurate financial information.

Critical areas not covered by this handbook

Project management

Apart from the SAP security and internal control considerations addressed in this handbook, there are other areas which must also be considered when implementing a SAP system. Project management of the SAP implementation is of critical importance in ensuring that the implementation of SAP is successful. Basic project management practices should be put in place, including the appointment of a project manager and a high level steering committee to oversee the project. The project should consist of various phases such as planning, design, configuration, testing, training, data conversion and post-implementation review. It is important that the project scope has been clearly defined and that team members become familiar with the complexity of the project. Internal Audit should be involved in all phases of the project, to monitor project risks and to ensure that adequate security and controls are considered and developed. Regular meetings should be held with project staff to discuss issues and concerns relating to the project.

In addition to the above, it is also important that the agency selects adequate ‘implementation partners’ (who are consultants that have been approved by SAP Australia to have technical expertise) to assist in the implementation of SAP. Implementation of SAP without the use of an implementation partner is difficult and may significantly increase the risk that SAP will not be implemented correctly, on time and within budget.

Some of the more significant risks which have resulted in difficulties in implementing SAP are:

• Misunderstanding of the complexity of the SAP project by project team members resulting in insufficient time being allowed to implement the system.
• Not using an implementation partner and instead trying to implement the SAP system ‘in-house’ without the necessary technical expertise.
• Trained staff leaving the project to become SAP consultants, making it difficult to replace them.
• SAP security and control structures not being adequately set up and tested before implementation.
• Certain project phases, such as user testing, not being adequately completed due to tight implementation deadlines.
• Lack of system documentation, making ongoing support and upgrades more difficult.
• Data conversion being considered too late in the project.
• Inadequate consideration given to business process redesign which may affect the level of change, complexity and overall project risk.

The SAP environment

For a completely secure system that can provide reliable financial information the environment that operates around SAP must be well controlled. This environment includes the operating system and the Database Management System (DBMS). The operating system can further be divided into the Local Area Network (LAN) operating system and the server operating system.

Typically a client/server environment consists of both an application and DBMS server networked to the client (ie. the desktop PC) through the LAN. In some cases the application and DBMS server can be one and the same. SAP resides on the application server with a Graphical User Interface or GUI residing on the client.

Security at all of these levels must be adequate to ensure that financial information obtained from SAP is accurate, complete and valid. For example, if security at the database level is poor, then unauthorised users may access and possibly corrupt or change the data stored in the DBMS. Clearly this affects data reliability. Similarly access to the operating system can provide a doorway to access the financial data. The control and security of operating systems will be the subject of other Australian National Audit Office (ANAO) better practice handbooks/guides. At present a guide to Windows NT security is being compiled and will be available in late 1998.

Applicability of the handbook to the ANAO financial statement audit

Depending upon the approach chosen by the ANAO to audit a particular balance in the financial statements, the controls within SAP may or may not be subject to review. The choice as to which audit techniques are to be employed rests with the auditor and is one of efficiency and effectiveness.

The approach may be either one where tests of control are performed to determine if the system of internal control is reliable (commonly known as a controls approach) or one where transactions making up a particular balance are examined and verified back to source documentation or vice versa (known as a substantive approach). Alternatively a mix of both types of procedures may be employed. During tests of controls not all controls will be tested. Only those that the auditor intends to rely upon will be evaluated.

Why is SAP security and control different?

SAP R/3 is a very complex integrated system which can be used to satisfy most of an organisation’s data processing requirements. The nature of SAP demands a different approach to addressing security and controls. The reasons for this include:
**Flexibility and breadth of functionality**

The SAP software is designed to be a total business solution for both financial and non-financial processes. The software covers more business functions than any other product on the market, this adds to the complexity of security and control issues. To achieve this total business solution, the software has been designed to be flexible and highly configurable. Amongst other things, it is necessary to configure:

- Validation rules and tables.
- Override capabilities.
- Calculation rules.

These are controlled via tables which can be configured to produce a well controlled environment, or alternatively a poorly controlled environment if configuration is not adequate.

**Complexity**

To provide a function-rich and flexible software solution, the SAP package has been developed using a table-driven approach. Most business functions can be performed in a multitude of ways in SAP. The various options available increase the complexity of the implementation and the risk of incorrect, inconsistent or uninformed decisions being made during the design phase.

**SAP is completely integrated**

All data within SAP is stored in a central database and the system provides seamless integration for data captured in one module but pertinent to another. Although this decreases the risk of incomplete transactions due to the self-balancing characteristic of SAP, it does present some additional risks:

- Access security is more complicated. With all information stored centrally, it is necessary to ensure that the data can only be viewed by those who are authorised to do so.
- Design decisions made for one SAP module might have an unexpected adverse impact on another module. Effective interaction within the project team is therefore essential.

**No traditional application / environment split**

In SAP the boundaries between users of applications and the IT department (programmers, operators and database administrators) are not clearly defined. Although segregation can be achieved through complex authorizations, many of the traditional non-user activities are performed within the application software (eg program changes, job scheduling, systems administration). This increases the risk of segregation of duties problems within SAP environments.

**Shortage of skilled resources**

Although SAP has been released on the Australian market now for several years, there is still a shortage of skilled resources for some of the new functionality included with the latest releases, including the use of profile generator, the Human Resources module and HR position-based security. This increases the risk of these features not being implemented to a satisfactory standard. Retention of staff who develop SAP skills during the course of an agency’s implementation project is also a significant issue which can have a serious impact on ongoing support, maintenance and effective use of the system.
How to read the better practice handbook

The handbook has been divided into eight sections covering the following:

• An introduction to the handbook.
• The various application modules.
• Basis module/cross-application matters.
• Appendices which contain an introduction to SAP concepts, and a glossary of terms used in the handbook.

Each application module has been divided into the major processes or functions (subsections) that are performed within that module. For example, the section dealing with ‘purchases to payables’ is split into purchasing, vendor master file, goods receipt, invoice verification, accounts payable, and payment processing. Each sub-section is introduced through a brief narrative followed by several components:

Significant risks specific to the function being addressed are summarised in a table. Each of these risks is addressed in detail in the following sections addressing ‘best practice procedures’.

Configuration 'Hot Spots' refer to the customising settings which are critical to achieving security and control best practices. You may need to refer to your SAP controls consultant or implementation partner regarding the specific settings required on your release of SAP R/3.

The handbook then discusses the key risk factors relating to the function and for each of these factors describes best practice procedures that should be considered to mitigate the risks. The handbook also provides a summary of the standard features contained in SAP R/3 that help address the risk factors.

The best practice procedures are coded to emphasise their importance:

### Critical

- Blue text is used for ‘best practice procedures’ considered critical to achieving an acceptable level of control. If these procedures are not in place, then there is a significant risk to the organisation.

### Important

- Black text is used for ‘best practice procedures’ which are considered important to achieving a good level of internal control but which, if not implemented, would not result in a high risk to the organisation.

### Desirable

- Italics are used for ‘best practice procedures’ which do not have a significant impact on the overall control environment but which may assist the control or efficiency of the business process.
For some of the ‘best practice procedures’ alternative controls may exist. Orange text is used for these potential compensating controls. Note that the alternative is generally not as strong a control as the best practice procedure.

This symbol indicates a potential compensating or alternative control.

Reports which are considered useful in ensuring that best practice procedures are followed are described together with the menu path and reporting tree used to access the reports.

The security section addresses some of the more significant factors that should be taken into account when implementing security for an application module.

Throughout the handbook it has been necessary to use a significant amount of SAP terminology. In order to assist the reader in understanding the concepts discussed in the handbook, terminology has been explained in a glossary contained in Appendix 2.

Note that the use of ‘authorization’ throughout the handbook refers to the SAP ‘authorization concept’ which is explained on page 190.

Introduction to SAP concepts

Reference has been made throughout the handbook to various SAP R/3 concepts. In order to assist the reader in understanding these concepts a brief introduction to some of the concepts fundamental to the SAP system has been included in Appendix 1. If you are not familiar with the basic SAP R/3 concepts, time should be taken to review this section before proceeding to read the handbook.
# Procurement to payables

## SECTION CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement cycle overview</td>
<td>11</td>
</tr>
<tr>
<td>Procurement/purchasing activities</td>
<td>11</td>
</tr>
<tr>
<td>Procurement/purchasing overview</td>
<td>13</td>
</tr>
<tr>
<td>Significant risks</td>
<td>14</td>
</tr>
<tr>
<td>Configuration ‘hot spots’</td>
<td>14</td>
</tr>
<tr>
<td>Purchasing data entry is accurate and complete</td>
<td>15</td>
</tr>
<tr>
<td>Purchasing documents are authorised</td>
<td>17</td>
</tr>
<tr>
<td>Useful reports</td>
<td>19</td>
</tr>
<tr>
<td>Security considerations</td>
<td>19</td>
</tr>
<tr>
<td>Vendor master file</td>
<td>20</td>
</tr>
<tr>
<td>Vendor master overview</td>
<td>20</td>
</tr>
<tr>
<td>Significant risks</td>
<td>21</td>
</tr>
<tr>
<td>Configuration ‘hot spots’</td>
<td>21</td>
</tr>
<tr>
<td>Changes to the vendor master file are authorised</td>
<td>22</td>
</tr>
<tr>
<td>Changes to the vendor master file are entered and processed correctly</td>
<td>23</td>
</tr>
<tr>
<td>Useful reports</td>
<td>25</td>
</tr>
<tr>
<td>Security considerations</td>
<td>25</td>
</tr>
<tr>
<td>Material master file</td>
<td>26</td>
</tr>
<tr>
<td>Material master overview</td>
<td>26</td>
</tr>
<tr>
<td>Significant risks</td>
<td>27</td>
</tr>
<tr>
<td>Configuration ‘hot spots’</td>
<td>27</td>
</tr>
<tr>
<td>Changes to the material master file are entered and processed correctly</td>
<td>28</td>
</tr>
<tr>
<td>Useful reports</td>
<td>29</td>
</tr>
<tr>
<td>Security considerations</td>
<td>29</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Receipt of goods/services</td>
<td>30</td>
</tr>
<tr>
<td>Overview of goods receipt</td>
<td>30</td>
</tr>
<tr>
<td>Significant risks</td>
<td>31</td>
</tr>
<tr>
<td>Configuration ‘hot spots’</td>
<td>31</td>
</tr>
<tr>
<td>Completeness of data entry</td>
<td>32</td>
</tr>
<tr>
<td>Receipts are matched against purchase orders and invoices</td>
<td>34</td>
</tr>
<tr>
<td>Useful reports</td>
<td>38</td>
</tr>
<tr>
<td>Security considerations</td>
<td>38</td>
</tr>
<tr>
<td>Invoice verification (Materials management)</td>
<td>39</td>
</tr>
<tr>
<td>Invoice verification overview</td>
<td>39</td>
</tr>
<tr>
<td>Significant risks</td>
<td>40</td>
</tr>
<tr>
<td>Configuration ‘hot spots’</td>
<td>40</td>
</tr>
<tr>
<td>Data entry is complete</td>
<td>41</td>
</tr>
<tr>
<td>Processing is complete</td>
<td>43</td>
</tr>
<tr>
<td>Invoices are authorised</td>
<td>47</td>
</tr>
<tr>
<td>Useful reports</td>
<td>48</td>
</tr>
<tr>
<td>Security considerations</td>
<td>49</td>
</tr>
<tr>
<td>Accounts payable (Financial accounting)</td>
<td>50</td>
</tr>
<tr>
<td>Accounts payable overview</td>
<td>50</td>
</tr>
<tr>
<td>Significant risks</td>
<td>51</td>
</tr>
<tr>
<td>Configuration ‘hot spots’</td>
<td>51</td>
</tr>
<tr>
<td>Data entry is complete</td>
<td>52</td>
</tr>
<tr>
<td>Processing is complete</td>
<td>57</td>
</tr>
<tr>
<td>Useful reports</td>
<td>59</td>
</tr>
<tr>
<td>Security considerations</td>
<td>60</td>
</tr>
<tr>
<td>Payment processing</td>
<td>61</td>
</tr>
<tr>
<td>Payment program overview</td>
<td>61</td>
</tr>
<tr>
<td>Significant risks</td>
<td>62</td>
</tr>
<tr>
<td>Configuration ‘hot spots’</td>
<td>62</td>
</tr>
<tr>
<td>Data entry is complete</td>
<td>63</td>
</tr>
<tr>
<td>Processing is complete</td>
<td>65</td>
</tr>
<tr>
<td>Payments are authorised</td>
<td>67</td>
</tr>
<tr>
<td>Useful reports</td>
<td>68</td>
</tr>
<tr>
<td>Security considerations</td>
<td>68</td>
</tr>
</tbody>
</table>
Procurement to payables

1 to 4 - Procurement/purchasing activities

The procurement process commences with determining the requirement for materials/services. A purchase requisition should be raised for all goods/services that the organisation procures. Requisitions may be raised with reference to a contract or outline agreement which specifies a certain volume of a material that should be purchased from a particular vendor. The system can also suggest an appropriate vendor for the material/service being procured via source determination (a vendor may be selected from a source list). 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. Where appropriate, the system should enforce a tender evaluation process via 'request for quotation' functionality.
Purchase orders can then be created based on the requisitions and any related quotations. Purchase orders should not be created without reference to a 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.

Master data relevant to the procurement cycle includes the vendor master and material master files.

5 - Goods receipt

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

6 - Invoice processing

Invoices are processed with reference to the appropriate purchase order and goods receipt transactions via the invoice verification transaction. Invoices that do not have a valid purchase order can be processed separately via the financial accounting accounts payable module. 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 relate to a valid purchase order in the system (e.g., utility payments) should be processed via the financial accounting accounts payable module. These invoices are not subject to the electronic approval enforced at the requisition stage and can be subject to authorisation controls at the invoice stage via payment release procedures used in conjunction with the ‘park and post’ functionality and SAP Workflow, to ensure that all invoices beyond a certain amount are authorised in accordance with approved delegation levels.

7 - Payment processing

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. 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. 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.
The procurement cycle commences with the determination of requirements. This may be performed by the system via materials planning and control and purchase requisitions generated automatically. Requisitions can also be raised manually and can be subject to an electronic approval procedure.

The requisition 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.
SIGNIFICANT RISKS

- Users may be able to specify delivery tolerances that would permit delivery of a significantly larger quantity of goods than were ordered (and approved).
- Key control settings may be modified online by the user to remove the need to process a goods receipt or invoice for a purchase order.
- Purchasing transactions may be performed without appropriate authorisation from management.
- Purchasing documents may be modified after being approved in the system.

CONFIGURATION ‘HOT SPOTS’

- Release strategies:
  - ensure they are complete. Gaps in the selection criteria for release strategies may mean that certain purchases are not caught by any strategy;
  - ensure release indicator ‘changeability’ settings result in orders/requisitions changed after approval (release) being subject to redetermination of release strategy and, if appropriate, reapproval.
- Use the purchase order parameter to prevent purchase orders from being created directly (ie. without referencing a requisition). Otherwise approvals via requisition release strategies can be compromised.
- Prevent overrides to over-delivery tolerances, payment terms and goods receipt indicators.
- Make use of purchase price tolerances.
Purchasing data entry is accurate and complete

During the purchasing process, all of the required data for the various purchasing documents (e.g., purchase requisition, purchase order) may not be entered correctly or some important data may be omitted from the purchasing documents. This could result in purchase orders being sent out to vendors with the wrong information.

Best practice procedures which could be implemented to ensure that all required purchasing data is entered correctly:

- 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 always required should be set to ‘optional entry’.

- Some fields are set as ‘required entry’ by SAP and cannot be changed (e.g., 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 (this field should be set as ‘display only’);
  - currency (for multiple currency companies);
  - account assignment;
  - under and over-delivery tolerances (these fields should be set as ‘display only’); and
  - GR control indicators (these fields should be set as ‘display only’).

- It is also possible to enter some 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.

- ‘Item category’ settings control the method of processing purchasing transactions in SAP. For example, it is possible to control whether an invoice receipt and/or material number is required for the transaction and whether or not a goods receipt is required. The ‘GR indicator binding’ parameter specifies whether a goods receipt is mandatory. This 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. It should be noted that this level of control can be achieved either via field status controls or item category configuration. It would not be essential to implement this control at both levels.

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.
SAP also has some standard features which help to ensure that purchasing documents are processed with information that is correct and to ensure that all required information is entered in the various purchasing documents:

- Information entered into SAP purchasing documents is automatically checked against specific master files including: vendor master data, material master data, and purchasing master data. Account assignment data is also checked (correct general ledger account). Attempting to process a transaction without entering data in a 'required' field produces an error message which must be corrected.

- Many of the fields in a purchasing document will have information that is entered by default from the material or vendor master record for the item or from a contract. As a result, the user does not have to enter data for some fields. However, this default information can be edited, and is checked for correctness by the system before the purchasing document can be saved.

- There are several methods used by SAP to determine which general ledger (G/L) accounts should be posted as a result of a purchasing transaction (goods receipt and vendor invoice), depending on the type of material/service being ordered:
  - if the materials ordered are inventory-type items for which a material master record is maintained on the system, SAP automatically determines which G/L accounts are updated during the goods receipt and vendor invoice transactions;
  - when ordering materials that do not have a material master record it is necessary to specify an 'account assignment category' in the purchasing document. The 'account assignment category' helps the system to identify the type of the accounts that must be charged when the goods/service receipt and vendor invoice are processed.

- 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.

- SAP warns the user if a duplicate purchase order has been entered into the system. The system will warn the user if a purchase order is entered with the same date, vendor and purchasing group. The user can then decide whether to extend the existing purchase order, or create a new one.

- Each purchasing transaction is recorded in the general ledger according to the date the goods are received and the goods receipt transaction processed in the system. The general ledger (financial data) is updated for the purchasing transaction when the goods are received.

- The vendor used in a purchase order is sourced from the vendor master file. The user can enter the vendor number or process a purchase order as 'vendor unknown' in which case the system provides a possible list of vendors ('source list'). A valid vendor and material must be entered before the purchase order can be processed.
Purchasing documents are authorised

Purchasing documents may be processed without being authorised if appropriate authorisation procedures are not enforced. This could result in unauthorised or fraudulent purchasing transactions being processed.

**Best Practice Procedure**

Best practice procedures which could be implemented to ensure that purchasing transactions are appropriately authorised:

- SAP can be set up to require the electronic authorisation of all purchase requisitions prior to further processing through the use of release procedures. Release procedures can be configured at a number of levels:
  - when a purchase requisition is created, the system can 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 require release for individual items or entire documents and varying levels of release criteria can be defined to ensure that purchasing documents are subject to the appropriate authorisation;
  - the system can be configured to define who is authorised to approve a purchase requisition and in what sequence this should be performed (e.g. purchasing manager followed by the financial controller);
  - the business process that follows the purchase requisition release can also be defined. For example, requisitions may be released to a purchase order or ‘RFQ’ or blocked from further processing;
  - the system can also be set to determine what happens if a purchasing document is changed during or after the release process. It is possible to control whether a change is allowed and whether a changed document will be subject to a further release procedure as a result.

- A different release authority can be assigned to individual users/positions within the organisation so that a purchase requisition can only be approved by a user with the appropriate authority levels. Release strategies should be established to reflect the levels of delegated authority within the organisation.

**Important**

- Release procedures 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.

- In some SAP versions, purchase order release only prevents the printing/communication of the purchase order. However, it is still possible to process goods receipts and invoices and generate...
payments for an unreleased purchase order. Unreleased purchase orders should be monitored to ensure that any receipts/invoices processed for unreleased orders are followed up and appropriate corrective action taken.

- A parameter may be assigned to users to prevent the raising of a purchase order without reference to a requisition. The parameter enforces the use of the 'create PO with reference to a purchase requisition' transaction and can be used to prevent a user bypassing the release strategies at the requisition stage. If the user parameter is used it is also essential to ensure that users do not have access to maintain (and therefore remove) their own user parameters.

  If the user parameter is not activated, an alternative measure would be to develop an exception report for management review, listing all orders raised without a corresponding purchase requisition.

- After a purchase order has been created it is distributed to the vendor through the 'output process' (the order can be output to printer, fax or via EDI). 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).

- Purchase order details may differ from or exceed the approved requisition amount. A custom exception report may be developed to provide information for management review of orders where details differ from the requisition.

**Desirable**

- *The system allows an 'automatic authorization check' to be performed for general ledger accounts. This will check whether the user has authority to post to the general ledger account, which has been entered in the purchasing document. If the user does not have the appropriate authority in the system, they will be unable to process the purchasing document using the G/L accounts specified.*

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that purchasing documents are only processed if they have been appropriately authorised:

- A purchase order can be created manually in SAP via two different methods. If the vendor/supplier details are known, the user can simply enter the existing vendor name or number into the system and all relevant information will be retrieved from the vendor master files. If the vendor/supplier details are unknown, the system will present a list of possible vendors (called a 'source list') for the material ordered. The user can then select an existing vendor for the material. However, for each method of ordering, the vendor details are checked by the system against the vendor master file.

- Purchase orders can be created based on an existing purchase requisition. A purchase requisition can only be used to create a purchase order if it has been released/approved online (this involves authorisation by an appropriate user).
USEFUL REPORTS

There are a number of standard reports available on the system which should be reviewed on a regular basis to ensure that purchasing transactions are adequately monitored and long outstanding purchase orders followed up. These reports can be executed via the menu path Information systems ➔ Logistics ➔ Purchasing ➔ ... or via the path Information systems ➔ General report selection. The following reports may be useful in monitoring the purchasing function:

- 'Purchasing documents by vendor/PO number/material etc.' - this report allows you to select all purchasing documents meeting the selection criteria and could be useful in monitoring open purchase orders (no goods receipt or invoice received);
- 'Purchasing document changes' - this report provides a listing of changes that have been made to the specified purchasing document including new and old values as well as details of the user who has processed the change. It may be useful in tracking changes for purchasing documents. A similar report is available for purchase requisitions;
- 'Purchase order price history' - a useful report to review the price history of purchase orders raised for selected vendors/materials. Also allows analysis of purchasing info records; and
- 'Display info record changes' - displays changes made to purchasing info records and may be useful to review info record changes to ensure they are authorised.

SECURITY CONSIDERATIONS

- There are several 'authorization objects' that are used to restrict access to purchasing transactions. Particular attention should be paid to the following objects, which should be used to ensure that release procedures are implemented and assigned to users according to the delegation authority limits within the organisation:
  - 'Release code and group (purchasing)' - this is used for release procedures that have been defined with complex delegation structures (with classification); and
  - 'Release code in purchase requisition' - used for release procedures that have been defined using simpler release criteria.
- Users should be assigned the relevant release codes to ensure they can release only those requisitions/orders for which they are authorised.
- Consideration should also be given to restricting access to purchasing functions by purchasing organisation, purchasing group, plant and document type to ensure that only authorised users can process purchasing documents in the system.
- Appropriate consideration should be given to segregating conflicting duties in the purchasing function. For example, users should not have access to raise purchase requisitions and release the same requisitions. Functions of master data maintenance (vendor, material master files) should also be separated from purchasing functions. Purchasing users should also be restricted from performing other functions in the 'purchases to payables' business process including processing of goods receipts, invoice entry, and generation of payments.
Vendor master file

Vendor master overview

The vendor master file is used to store information about each of the vendors from whom the organisation purchases materials. Data is stored at three levels in the vendor master file: general data that relates to every company code and purchasing organisation; company code/accounting data that is specific to each company code; and purchasing organisation data that is used in the raising of purchasing documents.
**SIGNIFICANT RISKS**

- Payments are able to be processed for an alternate payee that is entered into the system during invoice processing.
- One-time vendor accounts are able to be created which could allow the processing of invoice documents for one-time vendors (vendor and bank data is entered during invoice processing).
- Unauthorised changes to bank account details may result in misappropriation of payments.

**CONFIGURATION ‘HOT SPOTS’**

- The system should be configured to ensure that an alternate payee cannot be directly entered into the invoice document.
- The error message for highlighting potential creation of duplicate vendors should be activated via message control.
- The duplicate invoice check flag in the vendor master record should be mandatory, to ensure that duplicate checking is activated for all vendors.
- Authorization groups may be used, if appropriate, for securing access to certain groups of vendor master records (e.g., if employee vendors are established for expense reimbursement). Optional security will need to be activated in order to implement this level of control.
Important

Vendor master files may be created or changed without the appropriate authorisation. This could result in fraudulent vendors being created on the system or changes being made to critical vendor data such as address or bank details.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that changes to vendor master records are authorised:

- The system documents all changes to master records and documents. Standard reports are available to query this information.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that changes to vendor master records are authorised:

**Critical**

- Access to vendor master maintenance should be restricted. Refer to ‘Security considerations’ on page 25.
- An independent review should be performed of audit trails for changes to vendor master records. Refer to ‘Useful reports’ on page 25.

**Important**

- The system can be configured to check for duplicate records when creating customers and vendors. A message appears that the address is the same, and the user should check for a duplicate. A list of potential duplicates appears, and the user can display the individual records to check for actual duplicates. This message should be activated for online entry.
- Procedures should also be implemented to ensure that a search for potential duplicates is performed prior to creating each new vendor master record. Searches may be based on ‘search term’ or ACN for example.
Changes to the vendor master file are entered and processed correctly

Information required in the creation/maintenance of a vendor master record may not be completely entered into the system, resulting in erroneous vendor data stored on the system.

**BEST PRACTICE**

**PROCEDURE**

Best practice procedures which could be implemented to ensure that vendor master records are entered for correct processing:

• Required fields should be properly configured in the vendor master records as appropriate. The following key fields should be set to 'required entry':

  **General data:**
  • name1;
  • search term;
  • street;
  • postal code;
  • country;
  • language; and
  • bank.

  **Company code data:**
  • reconciliation account (control account in the general ledger);
  • payment terms;
  • check double invoice; and
  • payment methods.

  **Purchasing data:**
  • order currency; and
  • payment terms.

• The 'Alternate payee in document' field in the vendor master records (General data section) should be set to 'suppressed'. This field allows entry of an alternate payee in the invoice document during invoice processing, and therefore removes the control of having an independently maintained vendor master record.

• Use of one-time vendor accounts should be strictly controlled as these allow address and bank data to be entered for the vendor in the invoice document at the time of processing. Refer to the detailed discussion in the 'Accounts payable' section.

• An independent review of the audit trail for changes to vendor master records may be performed and changes verified against the approved amendment form.
Important

• If evaluated receipts settlement (ERS) processing is used it must be activated in the vendor master record as well as in the purchasing info 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 can 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.

• Payment terms are specific agreements with customers on how the 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.

• 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.

Desirable

• Naming conventions should be used to ensure the same vendor details have not been created under different names (eg DOF or D.O.F.). The field ‘search term’ can be used as a useful means of restricting searches for existing vendors.

SAP also has some standard features which help to ensure that vendor master data is completely and accurately entered for processing:

• The system documents all changes to master records and documents. Standard reports are available to query this information.

• Many of the important vendor master data fields are mandatory fields during data entry.

• Every master record must be assigned to an ‘account group’. The account group controls the:
  ○ numbering for each type of master record based on an internally (system generated) or externally (user) assigned number range. Vendor master records are assigned a unique vendor number;
  ○ fields that will appear on the screens when creating a vendor record along with their data entry status (required, optional, suppress, or display only).
USEFUL REPORTS

There are several standard reports available on the system which should be reviewed on a regular basis (eg weekly) to ensure that all changes to vendor master records are reviewed and authorised:

- 'Display of vendor changes' - 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' - this report provides details of all new vendor master records created for the selected date range; and
- 'Vendor master record comparison' - this report highlights any vendor master records that might have incomplete information that is required for purchasing functions.

The report 'Display of bank changes' should also be reviewed regularly to ensure that changes made to bank master data are authorised.

A number of useful reports are also available for review of changes to standing data for vendors. These reports should be reviewed on a regular basis to ensure that changes are appropriate:

- 'Price change for vendor’s info records' - provides a review of price changes made to vendor’s info records. The report supports a number of selection criteria to refine the search;
- 'Price change for vendor’s contracts' - as above but for contracts; and
- 'Price change for vendor’s scheduling agreement' - as above but for scheduling agreements.

SECURITY CONSIDERATIONS

- The optional authorization object 'Vendor: Change auth for certain fields' can be used to restrict access to groups of fields on the vendor master records.
- It is possible to restrict the range of vendors that a user can maintain using the optional authorization object 'Vendor: Account auth'. Vendor master records can be assigned to authorization groups and then users allocated authority for specific authorization groups. This could be used to separate maintenance access for sensitive vendor accounts (eg employee vendor accounts). This object must also be allocated in conjunction with the corresponding accounting document object.
- Authorizations can also be used to restrict which master data maintenance views can be accessed (accounting or purchasing). This is controlled by the authorization object 'Vendor: Application auth'.
- Appropriate consideration should be given to segregating conflicting duties in the procurement cycle. Refer to 'Procurement/purchasing activities' section for further details.
The material master file is used to store the materials that are purchased by an organisation. A material master record can be 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. Not all views will be used by all organisations. 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 handbook. However, the material master file is covered briefly to provide a more complete picture of the procurement process.
SIGNIFICANT RISKS

• Material master records do not contain all the required information ‘views’ necessary for the complete processing of material transactions.
• Unauthorised access to the material master file could result in inaccurate updates to standard costs.

CONFIGURATION ‘HOT SPOTS’

• Appropriate under- and over-delivery tolerances should be configured for the purchasing value keys assigned to material master records, to prevent excessive over-deliveries.
• Negative stocks should be disabled unless specifically required for a particular material type.
• Ensure that the automatic generation of purchase orders is appropriately configured in all master records.
• A source of supply for each material should be maintained for source lists.
Changes to the material master file are entered and processed correctly

Changes to the material master file may not be processed completely, resulting in a loss of data integrity.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that changes to the material master file are processed accurately and completely:

**Critical**

- 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.

- Procedural controls should be implemented to ensure that all necessary material master information is input during the creation or maintenance of master records. Fields which are required should be set as 'required entry' fields via field status configuration.

**Important**

- The system can be configured to prevent negative stock balances.

  SAP can be configured to permit negative stocks for standard-price materials. The use of negative stocks is best avoided, but may be legitimate in some instances (e.g., goods issue of stock that has not yet been receipted but is sitting in the warehouse). However, the system expects physical stock movements to be entered at a later stage. If considered necessary, the use of negative stocks should be limited and procedures should be implemented to ensure that there are no negative stocks remaining at balance date.

- Materials should be defined to be managed by quantity and value to ensure that both quantities and stock values are maintained by the system.

- It is possible to configure the system to permit the automatic generation of purchase orders from requisitions. If this functionality is used, care should be taken to ensure that the vendor and material master files are appropriately set.

- 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.

- Procedures should be implemented to ensure that appropriate searches are performed on the material master file prior to creating a new material master record, to avoid potential duplicate records.

- The standard audit trail report for changes to material master records should be independently reviewed on a regular basis to ensure that all changes are authorised and accurately performed.
SAP also has some standard features which help to ensure that changes to the material master file are processed accurately and completely:

- The material master file is the central repository of material information (such as stock levels) for the company. It assists in avoiding duplication and redundant inventory management data.
- Accounting data for the material master record is mandatory if the material type indicates that the material is managed by value in stock.
- Material type determines which information/views can be maintained for a given material (e.g., no sales data can be maintained for a raw material).

USEFUL REPORTS

- SAP offers a standard audit report of material master data changes. This report should be reviewed by the owners of the material master data on a regular basis.

SECURITY CONSIDERATIONS

- Authorization 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’.
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. Tolerances can be used to limit over- and under-deliveries of ordered goods.
**SIGNIFICANT RISKS**

- Access to process a goods receipt without reference to a purchase order may allow the matching controls to be bypassed.
- Users may be able to process a goods receipt for a quantity in excess of the actual quantity ordered.
- Goods may be receipted into 'blocked stock' resulting in stock being held without a value in the general ledger.
- Users may be able to process entry of initial stock balances, which is a data conversion transaction only.
- The goods receipt step may be bypassed if certain flags are set on the purchase order.

**CONFIGURATION ‘HOT SPOTS’**

- Reason codes should be enforced for return/write-off transactions.
- Movement type settings for consumption postings should be appropriate.
- Purchasing value keys should not be configured to permit excessive over-deliveries.
- The delivery should be automatically flagged as 'complete' if it is within the under-delivery tolerances.
- Reversal of a goods receipt once the invoice has been processed should not be permitted.
**Completeness of data entry**

Details of the goods receipt/service transaction may not be completely entered into the system. This may prevent the system from matching the invoice against the relevant PO and may prevent the G/L accounts from being updated.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that all goods receipt/service data is entered for processing completely:

**Critical**

**Goods receipt processing:**

- Tolerances can be configured to ensure that only reasonable differences are allowed between the goods receipt and purchase order quantity, and between the goods receipt and material master data. Variances can be defined for purchase order price quantity and for the moving average price. The purchase order price quantity variance can be set at different levels as a warning and error message. These should be set to appropriate values for the organisation.

**Important**

**Goods receipt processing:**

- 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.

- The GR/IR reports available in the system (refer to 'Useful reports' on page 38) should be reviewed periodically (eg monthly) to ensure that any unmatched invoices (eg if the goods receipt has been omitted) are followed up.

- A regular review should also be performed for any long outstanding purchase orders which are awaiting delivery. Refer to 'Useful reports' under 'Procurement/purchasing activities' on page 19 for further detail.

- Goods receipt quantities should be manually checked by receiving staff at the point of physical receipt and these should be verified against the details input. Periodic stocktakes should also be performed to ensure the accuracy of materials stored on the system.

**Service entry and acceptance:**

As noted for goods receipt processing, and

- 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. Service entry sheets may only be accepted by appropriately authorised users. SAP security can be set up to segregate the entry and acceptance functions. That is, one person is authorised to enter services performed; another is authorised to accept them. This effectively provides an electronic authorisation of the services for payment.
• ‘Planned’ services can be entered with precise descriptions. Alternatively, it is equally possible to enter just a money value limit covering ‘unplanned’ services. ‘Unplanned’ services are services whose exact nature is not clear at the time of the bid invitation phase. Entering value limits to cover such cases ensures that cost control can still be maintained.

SAP also has some standard features which help to ensure that all required data is entered during goods/service receipt processing:

**Goods receipt processing:**

- When a goods receipt transaction is processed, a valid purchase order number must be entered and matched by the system before further processing can occur. The purchase order number entered must be for an open purchase order (i.e., a purchase order which has not yet been fully receipted against).

- Fields are tested automatically for blanks, alphas, and values within a specified range. Data input which is not meaningful produces an error message, prohibiting processing until it is corrected.

- SAP keeps track of the undelivered PO quantity and automatically updates this quantity with the actual quantity received. This may be a partial delivery or a full delivery of the amount ordered. If the amount delivered exceeds the amount ordered, this may be rejected depending on the settings configured in the system (refer discussion on page 34).

- When a goods receipt is processed (for stock valued in the material master file), the stock balance in the GL and the stock subledger (in the Materials management module) is automatically updated with either the stock price as recorded in the PO or the price as defined in the invoice. The stock will automatically be updated with the actual cost when the vendor invoice is processed. SAP will automatically allocate the difference with the actual cost to the appropriate variance or cost of sales accounts according to the configuration of the system.

- A material document and an accounting document are generated by the system for each goods receipt transaction. The accounting document contains the general ledger posting information. SAP will allow the user to review the material documents and the accounting documents on a selective basis. These two generated documents form the basis to track transactions through the system.

**Service entry and acceptance:**

As noted for goods receipt processing, and:

- The service entry sheet is used to record services as they are actually performed by the vendor or subcontractor.

- For planned services, the services actually performed are recorded in the entry sheet with reference to the specifications already entered in the PO.

- For unplanned services (defined only in the form of money limits in the PO), the service entry sheet constitutes the document in which precise specifications are entered into the system for the first time.
Receipts are matched against purchase orders and invoices
Goods/service receipts data may not be matched to the relevant purchase order and invoice data. This may prevent payment processing from occurring.

**BEST PRACTICE PROCEDURE**
Best practice procedures which could be implemented to ensure that goods receipt transactions are completely processed and matched against the corresponding purchasing documents:

- If a valid PO number does not exist in the system, a delivery can be 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.

**Delivery tolerances**

**Purchase order quantity = 100 units**

- Under delivery tolerance 10% (70-89)
- Over delivery tolerance 20% (121-140)
- No message within the tolerance range (90-110)

- The goods/service receipt is compared with the quantity from the purchase order. The system assesses whether further processing is possible based on the tolerance limits recorded in the purchase orders. SAP will not accept a goods receipt quantity that exceeds the over-delivery tolerance, and will issue a warning for quantities entered that are below the under-delivery tolerance (refer diagram above). Quantities entered that are within the over-delivery and under-delivery tolerances are accepted by the system without a message. A quantity of goods received which is smaller than the order quantity minus the under-delivery tolerance is interpreted and accepted as a partial delivery. The tolerance limits are established in the material master records or purchasing info records and should default into the purchase order. Over-deliveries/under-deliveries can be controlled via the following:

  - Unlimited over-delivery indicator - allows a received quantity to be entered that is greater than the quantity ordered without any limit. In most organisations it is recommended that this should never be set.
• Over-delivery percentage - determines the maximum quantity of this item that will be accepted for delivery. Exceeding the tolerance percentage will result in an error. This should be set to zero or an appropriate value dependent on the material.

• Under-delivery percentage - determines the minimum quantity that will be accepted and treated as a complete receipt; the remaining quantity outstanding will be considered open. Exceeding the percentage will result in a warning and a partial delivery will be processed.

• Delivery complete indicator - shows the purchase order should be closed. If the quantity received is within the over- and under-delivery tolerances, this indicator is set automatically. This indicator can also be manually set.

- There are several types of goods receipt transactions in SAP. SAP allows goods to be receipted into ‘blocked stock’. This may be used if further inspection of the stock is required before accepting the delivery. However, processing a goods receipt into blocked stock does not update the value of inventory in the general ledger. Procedures therefore need to be implemented to ensure that an accrual is raised for the value of any blocked stock as part of month end closing.

- 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.

Important

- Purchasing value keys can be referenced on individual material master records to pick up default values for purchase orders for fields such as delivery tolerances. Permitted delivery tolerances should be defined via value keys and assigned to materials.

- The system should be configured to ensure that a reversal cannot be processed for a goods receipt (where ‘goods-receipt-based invoice verification’ is being used) 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 can properly reference and reverse the original data.

Desirable

- A description of why the goods were returned should be entered for returned deliveries to provide a sufficient audit trail for the transaction.

- The system can be configured to permit automatic creation of storage location data at the time the first goods receipt transaction is processed for a material. This should only be activated during data conversion. Storage location data should be created in the material master record in the live (production) system.
STANDARD FEATURES

SAP also has some standard features which help to ensure that goods/service receipts are matched against the relevant purchasing documents and invoices:

- A pre-existing purchase order (PO) number must be input to match against the receiving data.
- When the purchase order number has been entered, the purchase order details are retrieved and the open items/quantities from the purchase order are then proposed as the goods receipt data (copied into the goods receipt document). Line item information can be changed by the user to match the actual items/quantities received.
- The following fields are required for processing a goods receipt transaction:
  - movement type;
  - plant;
  - PO number;
  - vendor (if PO number is not known);
  - quantity received;
  - posting date; and
  - material.
- SAP does not allow erroneous goods receipt data to be deleted. Instead these must be reversed/cancelled.
- Unmatched goods/service receipts are saved by the system as open items in the GR/IR Clearing account. This account can be reviewed using the standard reports provided in SAP and should be regularly reconciled.
- Returned deliveries are validated against the original receipt and reversing entries are automatically created. Following the cancellation of a document, an exact opposite of the original document is automatically generated by SAP, cancelling the original accounting entries.
- A document date and posting date must be entered via the initial goods receipt screen. The system defaults the current date for both fields, both of which can be overridden. The user will receive a warning message if the document date is in the future. The posting date must fall within the current or previous posting (accounting) period, or the document will not be processed.
- If the goods/service receipt document passes all system edit and validation checks, it can be posted. This results in the creation of a material document which updates inventory balances and valuation (standard or moving average) in the material master record. The accounting document automatically posts to the general ledger accounts determined from the purchase order.
- SAP automatically posts to the correct general ledger accounts on the basis of parameters configured for each goods receipt/service receipt transaction type (eg goods receipt for PO; goods receipt for PO reversal).
- A GR/IR clearing account is used to accrue the liability for goods receipt. Goods receipt entries that cannot be matched to an invoice are maintained as open items in the GR/IR clearing account. During
invoice posting (IR), the vendor account is credited and the GR/IR account debited. GR and IR entries in the clearing account are matched and cleared. Various reports are available to analyse the balance of the GR/IR account.

- The delivery completed indicator is automatically activated if delivered quantity is within delivery tolerance settings. This indicates that the purchase order has been completely delivered and the purchase order is closed.
USEFUL REPORTS

There are several reports available in the SAP system which should be considered for use in monitoring the receipting function. These can be accessed via the standard reporting tree, menu path: Information system ➔ Logistics ➔ Inventory management ➔ .... Reports which may be useful in managing the receipting function include:

- 'Display material documents for material’ - provides a listing of all material documents according to the selection criteria, allowing selection by movement type. This report could also be used to provide a list of receipts that have been processed into blocked stock;
- 'Receipts/issues analysis’ reports - various reports available by plant, material, storage location, material group, material type, division and business area which allow reporting and analysis of goods receipt/goods issue transactions. These reports should be reviewed regularly; and
- ‘Purchasing documents for vendor’ - this report can be reviewed to obtain information on purchase orders with the expected delivery dates and may be useful in planning for anticipated deliveries. Purchasing document reports may also be used to follow up long outstanding purchase orders.

The system also provides a number of reports which can be used to review the GR/IR clearing account:

- ‘GR/IR clearing accounts analysis’ report - this report provides a summary of individual postings to the GR/IR clearing account; and
- ‘List of GR/IR balances’ - provides an overall summary of the GR/IR clearing account balances and should be reviewed on a periodic basis to ensure that any long outstanding amounts are cleared.

SECURITY CONSIDERATIONS

- Consideration should be given to restricting access to inappropriate movement types in the system via the MM: Inventory management authorization objects. Users should be provided with access to only those movement types required to perform their duties. In particular, access to data conversion movement types should be removed following the successful data load.
- No users should be allocated the movement type which allows the processing of a goods receipt without reference to a purchase order.
- Appropriate consideration should be given to segregating conflicting duties in the procurement cycle. Refer 'Procurement/purchasing activities' section for further details.
Invoice verification (Materials management)

Invoice verification overview

Purchase order  
Goods Receipt  
Material master  
Vendor master  
Conditions  
Invoice Verification  
Invoice Document  
G/L accounts  
Assets  
Cost centres  
Purchase order  
Material master

Invoice verification is the process of entering the invoice for the purchasing transaction. Invoice details are matched to the purchase order and goods receipt details. The system can also be set up to verify the invoice simply against the goods receipt details. Differences outside tolerances result in the invoice being blocked for payment. Invoices can also be entered without reference to a purchase order or goods receipt.

Evaluated receipts 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.
SIGNIFICANT RISKS

- The vendor number may be changed during invoice verification to be different to the vendor in the purchase order.
- Invoices may not match the corresponding purchase order and goods receipt, but may still be processed for payment.
- Invoices may be processed that do not relate to a valid purchase order in the system.

CONFIGURATION ‘HOT SPOTS’

- Tolerances should be configured to ensure that significant variations between the purchase order, goods receipt, and invoice are blocked.
- Tolerances should be set to prevent the processing of invoices through invoice verification that do not reference a valid purchase order.
- Field display characteristics should be modified to ensure that the vendor cannot be changed during invoice verification from the vendor on the purchase order.
- Blocking reasons should be appropriately configured to ensure that blocking cannot be manually removed for invoices blocked via invoice verification.
- It should not be possible to override payment terms during invoice processing.
Data entry is complete

Failure to enter all of the required data during invoice processing could result in invoices being matched against the wrong purchase orders or against the wrong general ledger accounts.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that invoices are entered for processing accurately and completely:

**Critical**

- During invoice verification, the user can enter a vendor number which differs from the vendor on the purchase order. A warning message is issued, but the invoice is accepted and not blocked for payment. The vendor number field should be set to prevent user input during invoice verification. The vendor details will be defaulted from the purchase order document. This will ensure that the vendor number cannot be changed.

**Important**

- In order to use the evaluated receipts settlement (ERS) function, the ERS parameter must 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 can be removed for any particular line item.

- If a vendor has been set to ERS, the user can 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. 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. There are standard reports available to assist in this function (refer reporting section for Procurement/purchasing activities on page 19).

- The GR/IR reports should be reviewed on a regular basis (eg monthly) to identify long outstanding unmatched good receipts.
STANDARD FEATURES

SAP also has some standard features which help to ensure that all invoice data is completely entered:

• During invoice verification, SAP automatically retrieves information from the purchase order and goods receipt transactions and proposes values on the screen. The user can overwrite this information if the invoice differs. Data entered in the invoice and credit note transactions is then validated against data held in master files, including:
  ○ material data (material name and measure, delivery tolerances, prices etc);
  ○ vendor data (vendor details including payment terms and delivery); and
  ○ accounting data (account name and type, posting types etc).

• Various fields are defined as ‘required entry’ during invoice verification, including document date and gross/net invoice value.

• If ‘goods-receipt-based invoice verification’ is used, the invoice cannot be recorded in the system before the goods receipt has been processed.

• When invoices without a goods receipt or purchase order are posted, the user enters the offsetting account to be credited. The system can be configured to block these invoices automatically.

• SAP will perform the following checks against the data entered before allowing the document entry to be processed further:
  ○ the system checks for any price / quantity variance; and
  ○ the document must be in balance. That is, the debit and credit entries must be equal.

• If ‘evaluated receipts settlement’ (ERS) is used, SAP creates an invoice document based upon information provided by the purchase order and the goods receipt data including:
  ○ order price specified in the purchase order;
  ○ the quantity and posting date entered on the goods receipt;
  ○ vendor details;
  ○ company code; and
  ○ fiscal year.

• The system automatically extracts and calculates tax, payment terms and discount rates from the purchase order details when ERS is used to process invoices.
Invoices which are not processed accurately and completely may result in failure to pay suppliers on a timely basis and payments for greater than the amount ordered and/or received.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that invoices are completely and accurately processed in the correct period:

- When processing an incoming invoice through invoice verification, the system checks each item for variances between the purchase order or goods receipt and the invoice. Tolerance limits can be defined in the system so that minor variances do not have to be investigated. If variances in an invoice item are within these limits, they are accepted by the system. If a tolerance limit is exceeded, the invoice will be posted but it will be automatically blocked for payment if it exceeds the upper tolerance limits. If the invoice is blocked, all the items are blocked. Even if the invoice only displays variances in one item, the whole invoice is blocked for payment. The following tolerance limits can be configured in the system:
  - Variances in an invoice item - block all invoices that do not match the purchase order and/or goods receipt within the defined tolerance limits:
    - quantity variance - allows tolerance limits to be set for differences between the purchase order and invoice quantity;
    - price variance - allows tolerance limits to be set for differences between the purchase order and invoice prices - based on individual order/invoice line items. Price variances can also be defined for estimated prices and planned delivery costs;
    - quantity/price variance - quantity and price variances can be defined to operate in combination;
    - item amount without order reference - this tolerance permits blocking of an invoice processed without reference to a valid purchase order. It should be activated and set to an upper limit of zero. This tolerance is activated in combination with the 'amount of an invoice item' variance (refer below);
    - schedule variance - prevents payment if the invoice is delivered early or late and the invoice amount is large; and
    - moving average price variance - compares new moving average price with the original price and the limits defined. If this variance is exceeded, the invoice will not be blocked. A warning message is displayed for the user.
  - Amount of an invoice item - all invoices above a certain absolute amount can be blocked for the company code, regardless of the variances defined above. The appropriate tolerances (for item amount with/without order reference) should then be set.
• It is possible to process an invoice through invoice verification without reference to a valid purchase order. Invoices without a purchase order reference are not subject to the three-way matching control and should be restricted to processing via FI Accounts payable only (refer to Accounts payable section). Processing of invoices without a purchase order reference via invoice verification can be prevented by activating the appropriate tolerance key and setting it to an upper tolerance limit of zero. This tolerance key should also be activated for the company code.

**Important**

• The GR/IR account identifies timing differences between the receipt of goods and the receipt of an invoice, and must be periodically cleared using the FI clearing program. The GR/IR account must 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 (refer 'Useful reports' on page 48).

• The system can be configured to block automatically a random sample of invoices processed via invoice verification. 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 some threshold value.

• Invoices can also be manually blocked. Manual blocks can be applied at the vendor master file level (ie all invoices for the particular vendor will be blocked) or at the individual invoice level. Procedures should be adopted to ensure that the use of manual invoice blocking is reviewed on a regular basis to ensure the appropriateness of the blocking.

• Reconciliation accounts should be defined to ensure integrity between the general ledger and the accounts payable subledger. Each vendor (subledger) account should then be attached to the correct reconciliation account. Direct posting to the reconciliation account is blocked.

**Desirable**

• Default exchange rates for foreign currency transactions can be stored in a system table. These rates are then used as the default rates in all foreign currency transactions. A maximum exchange rate limit can be established to highlight significant translation differences.
SAP also has some standard features which help to ensure that invoices are processed completely and accurately:

- Invoices are verified against purchase order data (if processed through three-way matching) held in the system. The system will automatically check differences against tolerance limits before allowing the invoice to be paid.

- When the invoice is posted, the goods received/invoice received (GR/IR) account is debited and the payable to the vendor is created. This debit must be cleared against the credit in the GR/IR account created when the goods receipt was posted.

- If there is a quantity variance where the quantity invoiced is larger than the quantity of goods received, and if there is no further goods receipt recorded by the system, the GR/IR account will not be cleared automatically. The invoice may be blocked for payment (depending on the tolerance levels configured).

- SAP will automatically perform the following calculations based on information held in the system unless manually overwritten:
  - tax charges (if applicable);
  - exchange differences; and
  - cash discounts.

- SAP performs online validation checks against master files and tables for invoice data entered. Errors must be corrected and resubmitted before further processing is allowed.

- Amendment of invoice records is controlled as follows:
  - key fields in the invoice record such as the vendor code, invoice amount, posting keys (debit/credit entries), fiscal year and the tax amount cannot be changed; and
  - users must reverse the document and re-enter the invoice if these fields need to be amended. Fields that may be amended after the invoice is posted include the hedged amount and rate and updating of the cheque number and EFT reference number. The invoice amendment function also allows users to block/release an invoice for payment.

- Reversing an invoice through the reversal entry functions will create a reversing document, transposing the original debit and credit amounts.

- The system performs edit and validation checks prior to further processing of document reversals. Documents can only be reversed if the following criteria are met:
  - none of the line items has been cleared (i.e., paid);
  - only vendor, customer, or general ledger items were entered in the original invoice;
  - the invoice was posted within the FI module; and
  - the invoice contains valid values.
• The following fields are required in order to process a reversal entry:
  ○ document number;
  ○ company code;
  ○ posting date;
  ○ posting period; and
  ○ void reason code (for cheque cancellations).

• If the posting period for the original document is closed, the posting date field can be amended to post the new document to the current period when processing an invoice reversal.

• The system checks accounts entered to ensure they are valid vendor accounts.

• The accounts payable subledger and general ledger are fully integrated within SAP. Posting to the vendor account will automatically post to the appropriate reconciliation accounts in the general ledger on a real time basis.

• Automatic postings for sales tax (if applicable), cash discount clearing and price variances are also generated and the posting records displayed.

• SAP automatically performs the required debit and credit entries for reversal documents.

• Posting of invoices updates:
  ○ vendor account balances;
  ○ general ledger accounts;
  ○ purchase order history file; and
  ○ material master file (if applicable).

• SAP requires the invoice total to be entered as a control total. The invoice document cannot be processed if the detail is out of balance with the control total. SAP provides a line item for delivery costs.

• For purchase orders that have a delivery cost line item, the purchase order will remain open until those charges are processed through invoice verification. For purchase orders without a delivery cost line item, but where delivery charges are billed, a delivery cost line item can be added during invoice verification.
Invoices are authorised

Unauthorised invoices may be processed, resulting in invalid payments to suppliers.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that invoices are authorised:

- Release of blocked invoices should be performed by a person independent of the invoice entry function.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that invoices are authorised:

- Invoices are authorised via the three-way matching process. Electronic approval at the purchase requisition/order stage is the primary approval control. Separate approval at the invoice stage is unnecessary (except where the invoice is blocked because of a mismatch outside tolerance limits).
USEFUL REPORTS

• Exception reports should be reviewed on a regular basis to ensure that outstanding/open invoices are identified and followed up. These reports can be executed via the standard report trees: (Information system ➔ Accounting ➔ Financial accounting ➔ Accounts payable ➔ Report selection ➔ ... ). Reports that should be reviewed on a regular basis include:
  
  ○ ‘List of cleared vendor items’ - this report provides information of vendor line items (invoices) that have been paid;
  
  ○ ‘List of vendor line items’ - lists all line items (invoices) for the selected vendors including outstanding and paid invoices;
  
  ○ ‘List of vendor open items’ - provides a list of outstanding/unpaid vendor invoices which should be reviewed to ensure that there are no long outstanding invoices; and
  
  ○ ‘Vendor open items - list of due dates’ - provides a listing of due dates for unpaid vendor invoices.

• A regular review should be performed of the GR/IR clearing account to ensure that goods receipts and invoice receipts are matched and processed on a timely basis. This account tracks differences between goods receipts and invoices, goods receipts with no corresponding invoices, or invoices with no corresponding goods receipts. It is therefore essential that it be properly monitored using the report ‘List of GR/IR balances’.

• A regular review should be performed to identify potential duplicate invoices. The vendor master records should be set up to detect automatically potential duplicate invoices (refer ‘Vendor master file’ on page 23). However, a standard system report is also available – ‘Invoice numbers allocated twice’. This report enables checking of potential duplicate invoices according to a number of selection criteria, including invoices processed on the same date, for the same amount, and/or with the same invoice reference number. Procedures should be established for the regular review of this report.

• A periodic review should be performed for all blocked line items/accounts to ensure that payments are not unnecessarily blocked and that all payments that should be blocked are in fact being prevented from processing. There are several reports which facilitate this review:
  
  ○ ‘List of blocked line items’ - this report lists all line items that are blocked for payment;
  
  ○ ‘List of blocked accounts’ - this report details all vendor/customer accounts that are blocked for posting.

• If ERS functionality is being used the ‘evaluated receipts settlement log’ should be reviewed each time an ERS receipt is processed. It provides details of the transactions settled as well as information about transactions that were not settled, with possible reasons for settlement failure.
SECURITY CONSIDERATIONS

- Consideration should be given to restricting access to invoice verification functions by company code and plant. Access to the authorization object 'Invoices: Blocking reasons' should also be restricted to ensure that only authorised users are able to release blocked invoices. It is critical that the releasing function be segregated from invoice entry, to ensure that the approval processes are not compromised.

- Appropriate consideration should be given to segregating conflicting duties in the procurement cycle. Refer to 'Procurement/purchasing activities' section on page 19.
Accounts payable (Financial accounting)

Invoices can 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 (e.g., utility payments). Since these invoices are not controlled via a matching process, additional authorisation controls need to be implemented.
SIGNIFICANT RISKS

• Users may process invoices for materials management vendors using the accounts payable function (FI) therefore bypassing the three-way matching controls.
• ‘One-time vendor’ accounts may be used to process invoices.
• Duplicate invoices may be processed through the system, resulting in a double payment to the vendor.
• Unauthorised invoices may be processed in the system.

CONFIGURATION ‘HOT SPOTS’

• Payment blocking reasons should be appropriately configured to prevent direct removal of payment blocks during a payment run or via the manual entry of payments.
• The field status settings for payment terms should be set to prevent override of payment terms during invoice entry.
• Release approval procedures should be used to control the electronic authorisation of invoices.
• Any amendments to document change rules may compromise control.
Data entry is complete

Accounts payable data may not be completely or correctly entered, resulting in postings to the wrong accounts and/or without all of the necessary data.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that invoices are entered and processed completely:

- Use of payment release procedures should be considered to ensure that invoices processed through FI accounts payable are appropriate. Refer to 'Security considerations' on page 60.

Invoices processed through FI accounts payable are not subject to the same level of control (matching) as invoices processed through MM invoice verification. It is therefore important to limit the vendors for which FI invoices can be posted. This could be achieved via several possible methods:

- Use of a vendor master flag and a ‘user exit’ to identify vendors which are ‘FI’ as opposed to ‘MM’ vendors. The ‘user exit’ routine could be coded to reject an attempt to process an FI accounts payable invoice for a vendor without the ‘FI’ flag contained in the vendor master record;

- Procedural controls might be implemented to restrict the processing of FI accounts payable invoices to FI-vendors only. This should be supported by a review-based procedure such as electronic authorisation of all FI invoices or manual review of all FI invoices processed (via a report), to ensure that only FI vendors are processed using FI accounts payable.

- It is possible to enter invoice details without an existing record in the vendor master file through the use of a one-time vendor account. This allows the user to enter the vendor details (name, address, bank account) into the actual invoice document. Use of the one-time vendor account should be restricted for the following reasons:
  - use of the one-time vendor account removes any control through having an independent vendor master maintenance function;
  - the risk of fraudulent payments being processed is increased;
  - it is inefficient; and
  - there is no record maintained of purchases against one time vendors. The best practice procedure is to prevent creation of one time vendor accounts.
Alternatively, if there is a valid requirement to process some one time vendor accounts, there should be procedures in place to perform a post-entry review of every invoice processed against the one time vendor account(s).

• The system will perform a duplicate payment check if the ‘check double invoice’ indicator has been activated in the vendor master file for the vendor being processed. The system provides the user with either a warning or error message if the invoice amount matches the amount of another invoice which has already been posted (or a supplier invoice which is already existing in the vendor account). The best practice procedure is to leave this message as a warning and to perform a regular review of the ‘Invoice numbers allocated twice’ report (refer to ‘Useful reports’ on page 59) to follow up any potential duplicate invoices. Configuring the message as an error may serve simply to encourage the user to change the reference field, whereas a warning message can be ignored and is therefore likely to be detected on the exception report.

**Important**

• Each different type of accounts payable transaction can be configured with the following settings:
  - sequential document number ranges defined for each year;
  - the type of account to be used for the transaction (eg vendor account);
  - the ‘authorization group’ which can be used to restrict access to the transaction type;
  - the corresponding transaction type to reverse the original transaction;
  - the transaction can be restricted for processing customer/vendor items only;
  - the transaction type can be configured to require a reference number (eg vendor invoice number); and
  - the transaction type can be configured to require that a text description be entered at the commencement of each transaction.

• If the park and post functionality is being used, invoices can be parked in SAP until they are electronically approved. Invoices may also be parked to obtain manual approval (depending on the business process implemented). The ‘parked invoice’ report should be reviewed on a regular basis to ensure that there are no long outstanding parked invoices on the system. Refer to ‘Useful reports’ on page 59.

• If the park and post functionality is being used consideration should be given to developing a ‘user exit’ to ensure that a user with the access to post an invoice cannot post an invoice that they have also parked (that is, they cannot perform both functions). A user exit will be required to enforce this level of segregation.

If the release procedures functionality is not being used, consideration should be given to developing an exception report for review or performing a post-entry review of all FI invoices processed.
The frequency and the run schedule for posting recurring invoice data can be configured as required. The recurring entry program (RSBD-CSUB) must be run periodically to create the necessary invoice postings. Details of the batch run should be reviewed through the recurring entry program.

The 'Compact document journal' should be reviewed on a regular basis to identify any changes to recurring entry original documents. This should be reviewed by management independent of the process to ensure the changes are authorised and appropriate.

All document reversals should be based upon appropriate authorisation and should be reviewed to ensure they are performed accurately and completely. There are standard reports available in SAP (e.g., Compact document journal) which can be generated to facilitate management monitoring.

'‘Held’ documents are not easily tracked, except by the user who originally entered the invoice. As a result, procedural controls should be implemented to ensure that held documents are followed up on a regular basis to prevent the accumulation of long outstanding invoices.

EDI invoices may be rejected if the master data settings are not maintained under the ‘business partner’ functions in the vendor master records or if the invoice contains inaccurate data. Procedures should be implemented to ensure this information is appropriately maintained and that rejected invoices are followed up and corrected on a timely basis. An exception report should be developed to assist in the identification and follow-up of any EDI invoices that have been rejected during the interface to SAP.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that invoices are entered completely:

- Data entered for invoice and credit note transactions is checked against data held in master files, including the:
  - vendor data (vendor details including payment terms and delivery); and
  - accounting data (account name and type, posting types etc).

- The following fields are configured as ‘required entry’ fields and must be entered during accounts payable invoice processing. These fields are checked by the system to ensure the data entered is appropriate:
  - document date;
  - document type;
  - company code;
  - posting date (validated against open posting periods);
  - currency;
  - document number;
  - posting key; and
  - account number.
• The ‘posting key’ (debit or credit code) entered during FI invoice processing determines the treatment of the accounting entries in the general ledger (account assignment). The posting key is entered by the user and must be compatible with the account type of the transaction and general ledger account used.

• The terms of payment should be specified in the vendor master record. The terms of payment will then be defaulted into the invoice and should not be changed by the user during invoice entry. These terms are then used by the payment program. The payment terms control when the vendor will be paid.

• SAP enforces the balancing of all debit and credit entries for general ledger account line item entries.

• SAP will automatically perform the following calculations based on information held in the system unless manually overwritten:
  ○ tax charges (if applicable);
  ○ exchange differences; and
  ○ cash discounts.

• Exception reports are available within the system to identify outstanding / open invoices. Refer to 'Useful reports' on page 59.

• The combination of SAP document type, posting key and account number used to post an accounts payable invoice must be consistent.

• SAP allows the user to enter invoice data and either ‘park’ or ‘hold’ the data until the invoice can be completed. The invoice is only parked or held temporarily before it can be released for further processing and posting to the relevant general ledger accounts.

• Edit and validation checks performed for parked documents include the following:
  ○ Key fields are checked to ensure they are correct, including:
    ~ posting key (determines whether the line item is a debit or credit and the field status settings to be used for the line item); and
    ~ account number (verifies that the vendor account/general ledger account entered is correct and can be used with the posting key selected).
  ○ Fields that are normally defined as ‘required entry’ according to the posting key and account will be set to ‘optional entry’ fields. However, these will still be required entry before the document can be posted to the general ledger.
  ○ The system performs various ‘validation’ checks to ensure only reasonable data is entered. SAP will perform a full validation check when the document is posted/released.

• Parked documents do not update any transactions within the system until they are released/posted.

• Recurring document entries are automatically created and posted to the general ledger after running the periodic recurring entry programs.
• Each automatic batch run for recurring entry documents will create one document and update the following areas:
  o recurring entry original document;
  o next run date; and
  o total number of programs run.

• Before processing a reversal entry through the system, the following edit and validation checks must be satisfied:
  o there must be no cleared items for the document being reversed (ie none of the line items in the document can be paid);
  o only vendor, customer or general ledger items were entered on the original document;
  o the original document was posted within the FI module; and
  o the original document contains valid values.

• The following fields must be entered when processing a reversal transaction:
  o document number;
  o company code;
  o posting date;
  o posting period; and
  o void reason code (for cheque cancellations).

• EDI invoices can be processed into SAP in one of two ways:
  o the invoice/credit memo is parked using the preliminary posting function and then posted after it has been checked by the accounts payable clerk; or
  o the invoice/credit memo is posted directly to the general ledger provided no errors occur.

• The system automatically checks EDI invoices when they are released by users or posted directly to the general ledger. Errors identified during the interface are rejected for follow up and correction.
PRODUCTION TO PAYABLES

Desirable

• **Default exchange rates for foreign currency transactions can be stored in a system table. These rates are then used as the default rates in all foreign currency transactions. A maximum exchange rate limit can be established to highlight significant translation differences.**
STANDARD FEATURES

SAP also has some standard features which help to ensure that invoices are processed completely and accurately:

- Amendment of invoice records is controlled as follows:
  - key fields in the invoice record such as the vendor code, invoice amount, posting keys (debit/credit entries), fiscal year and the tax amount cannot be changed; and
  - users must reverse the document and re-enter the invoice if these fields need to be amended.
  Fields that may be amended after the invoice is posted include the hedged amount and rate and updating of the cheque number and EFT reference number. The invoice amendment function also allows users to block/release an invoice for payment.

- If the posting period for the original document is closed, the posting date field can be amended to post the new document to the current period when processing an invoice reversal.

- The accounts payable subledger and general ledger are fully integrated within SAP. Posting to the vendor account will automatically post to the appropriate reconciliation accounts in the general ledger on a real time basis.

- Posting of accounts payable invoices updates:
  - vendor account balances; and
  - general ledger accounts.
USEFUL REPORTS

- Regular post-entry review should be performed for invoices processed through FI accounts payable, including one-time vendor invoices and large value invoices. The ‘Compact document journal’ provides an audit trail of all transactions processed through SAP and would be useful for this type of review. It includes a range of selection criteria including transaction/document type.

- Exception reports should be reviewed on a regular basis to ensure that outstanding/open invoices are identified and followed up. These reports can be executed via the standard report trees: (Information system ➨ Accounting ➨ Financial accounting ➨ Accounts payable ➨ Report selection ➨ ... ). Reports that should be reviewed on a regular basis include:
  - ‘List of cleared vendor items’ - this report provides information on vendor line items (invoices) that have been paid;
  - ‘List of vendor line items’ - lists all line items (invoices) for the selected vendors, including outstanding and paid invoices;
  - ‘List of vendor open items’ - provides a list of outstanding/unpaid vendor invoices which should be reviewed to ensure that there are no long outstanding invoices; and
  - ‘Vendor open items - list of due dates’ - provides a listing of due dates for unpaid vendor invoices.

- A regular review should be performed to identify potential duplicate invoices. The vendor master records should be set up to detect automatically potential duplicate invoices (refer to ‘Vendor master file’ section). However, a standard system report is also available - ‘Invoice numbers allocated twice’. This report enables checking of potential duplicate invoices according to a number of selection criteria, including invoices processed on the same date, for the same amount, and/or with the same invoice reference number. Procedures should be established for the regular review of this report.

- The ‘Parked document vendor items’ report should be reviewed on a regular basis to follow up all outstanding parked documents on the system to ensure they are processed on a timely basis.

- A periodic review should be performed for all blocked line items/accounts to ensure that payments are not unnecessarily blocked and that all payments that should be blocked are in fact being prevented from processing. There are several reports which facilitate this review:
  - ‘List of blocked line items’ - this report lists all line items that are blocked for payment; and
  - ‘List of blocked accounts’ - this report details all vendor/customer accounts that are blocked for posting.

- Change document reports can also be reviewed for invoices to assess changes made to individual documents to ensure they are appropriate.
SECURITY CONSIDERATIONS

• Consideration should be given to restricting access to accounts payable functions by company code, business area, document type, and account type. Access to the authorization object ‘Invoices: Blocking reasons’ should also be restricted to ensure that only authorised users are able to release blocked invoices.

• Payment release procedures may be implemented using SAP workflow to enforce an electronic authorisation of FI accounts payable invoices. If a payment release procedure is defined, the system applies a payment block to the invoice which can then only be released by a user with the appropriate release authority. Vendor/customer master records are assigned to release approval groups, and release approval paths are used to define which users are responsible for approving a blocked invoice. Criteria include release approval group, document type, and amount. It is also possible to implement multi-level release (ie more than one person is involved in the approval process). The use of payment release procedures should be considered as an effective means of ensuring that all FI accounts payable invoices are appropriately authorised.

• It is possible to limit the vendor accounts that a user can post to, using the optional authorization object ‘Accounting document: Account authorization for vendors’. Use of this control feature should be considered to further secure the invoice processing functions.

• Appropriate consideration should be given to segregation of conflicting duties in the procurement cycle. Refer to ‘Procurement/purchasing activities’ section for further details.

• Limits can be defined to limit the amounts that users can post 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.

• Various tolerances and settings can be defined for vendors/customers to control clearing (payment) procedures, set limits for payment differences, specify how residual payment items (under- or over-payments) are to be treated, and set tolerance limits for the creation of residual items. These settings should be appropriately configured.
Payment processing

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.
**SIGNIFICANT RISKS**

- Users are able to release manually invoices that have been blocked due to a mismatch between the purchase order, goods receipt and invoice.
- Manual cheques can be processed online for an amount greater than the unpaid invoices that exist for the vendor on the system.

**CONFIGURATION ′HOT SPOTS′**

- Ensure payment blocking reasons prevent the inappropriate removal of payment blocks.
- Minimum payment values should be set at an appropriate level for each payment media type.
Data entry is complete
Payments data is not entered completely, resulting in inaccurate or incomplete payment processing.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that payments are entered for processing completely:

**Important**

- 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;
  - minimum payment amounts can be defined per payment methods; and
  - the bank accounts which can be used.

- 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.

- 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).

**Desirable**

- Cashed cheque data from the bank should be loaded via the standard SAP programs provided. Separate programs are provided for both electronic and hard-copy cashed cheque information.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that payments are entered for processing completely:

- Supplier invoices are automatically processed for payment if specific criteria are satisfied, including:
  - the invoice matches the purchase order/goods receipt within the defined tolerance limits;
  - the vendor is not blocked for payment; and
  - the invoice is not manually blocked for payment.

- Invoices are flagged once they have been paid to ensure that the payment cannot be duplicated. The ‘Payment proposal list’ provides details of each individual document which is due for payment. It can be reviewed online or printed out.
• SAP automatically assigns a clearing document number and clearing date when open invoice items are paid.

• Required input when generating the payment proposal includes the following:
  ○ company codes;
  ○ account types;
  ○ desired posting date;
  ○ payment methods; and
  ○ date of the next payment run.

• The following fields are required for generating a manual cheque payment:
  ○ company code;
  ○ payment method;
  ○ house bank;
  ○ printer for cheque and payment advice generation;
  ○ amount; and
  ○ value date.

• Manually created cheques are entered through the document entry program in accounts payable. Once posted, the payment document number must be allocated to the cheque number. Information required includes:
  ○ payment document number;
  ○ cheque number; and
  ○ fiscal year.

• Invoices are automatically selected for payment by SAP unless they have been blocked for payment.
PROCUREMENT TO PAYABLES

**Processing is complete**

Payments data may not be processed completely resulting in incorrect payments being sent to vendors.

**BEST PRACTICE PROCEDURE**

*Best practice procedures which could be implemented to ensure that payments are processed completely and accurately:*

**Critical**

- 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.

**Important**

- Cheque ‘lots’ (number ranges) for manual cheques should be defined in the system and should correspond with the cheque numbers printed on the stationery.

- Payment program reports should be reviewed during each payment processing run to ensure that all payments are processed completely and on a timely basis. The payment proposal list and the payment exception list should be reviewed to identify any invoices that are blocked for payment and to ensure no unauthorised payments are processed.

- Automatic postings define the accounts that are updated when payments are processed via the payment program. These should be set up to ensure the appropriate accounts are updated.

- The bank reconciliation should be prepared and reviewed by an independent person on a regular basis (eg monthly) using the functionality available in SAP.

- The accounts payable subledger should be reconciled to the general ledger control accounts on a regular basis (eg monthly). Vendor master accounts may be assigned to the incorrect control accounts. The reconciliation should be performed to ensure these accounts are identified and corrected on a timely basis.

- Errors occurring through cheque printing are recorded in the error log, which should be reviewed and cleared frequently. Errors can be corrected through various SAP utility programs available.

- The ‘Invoices numbers allocated twice’ report should be reviewed on a regular basis to ensure that no duplicate invoices are being paid (refer to ‘Useful reports’ page 48).
A register of manual cheques processed should be maintained and all manual cheque payments should be reconciled to the register to ensure that no unauthorised payments are processed. Appropriate physical security controls should also be in place over the safeguarding of blank cheques.

**Desirable**

- For unusual terms of payment the system can be configured to block payment automatically to enforce a review process prior to payment. Reasons for blocking payment can be defaulted based upon the terms of payment in the vendor master record. When posting to a vendor account, the blocking reason is proposed with the terms of payment.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that payments processing is performed completely and accurately:

- When an invoice is entered and released for payment based on the SAP three way match, the invoice is flagged for payment and will be automatically paid by the payment program according to the payment terms.
- Payment transactions can only be posted into SAP when the posting period is open.
- When the payment is made, general ledger accounts are updated automatically to reflect the transaction.
- Upon entry of the invoice, the system issues a message if there are any down payments in the vendor account that have not yet been cleared against an invoice. The system does not clear the outstanding down payment within the vendor account automatically. An appropriate manual review should be performed to ensure that all down payments are cleared.
- Postings in accounts payable are simultaneously recorded in the general ledger, with different accounts being updated according to the transaction involved.
- When the SAP batch payment program processes a payment, it automatically clears the open invoices being paid. The next payment run will only include ‘uncleared’ items for payment.
- When the batch payment program is run SAP proposes a list of all outstanding invoices, with a status field indicating whether the invoice is blocked for payment.
- An invoice is flagged after being paid to ensure that the payment cannot be duplicated.
- In order to clear open (unpaid) invoices SAP requires the following criteria to be met:
  - the sum of the line items entered equals the sum of the activated open items (debits equal credits); or
  - differences between the debits and credits are within a tolerance limit configured in the system.
- Details of discount rates are either defaulted from the vendor master or can be entered in at the invoice entry stage. The system automatically calculates appropriate entries for discounts and translations of foreign currency upon input of required data, eg value dates, discounts and exchange rates. The discounts for early payment are calculated automatically from the payment terms.
Payments are authorised

Payments may be processed which are not for authorised invoices.

**BEST PRACTICE PROCEDURE**

*Best practice procedures which could be implemented to ensure that system payments are authorised:*

**Critical**

- 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.

**Important**

- The approval limit for the amount a user can release for payment can be configured to restrict the release of unusually large payments.

**STANDARD FEATURES**

*SAP also has some standard features which help to ensure that payments are authorised:*

- The payment program automatically pays any open items (unpaid invoices) which are posted in the system. The payment is authorised at the point of invoice entry.
USEFUL REPORTS

The payment program reports should be reviewed as part of payment program processing to ensure that all payments are authorised. Particular attention should be paid to large or unusual payment amounts as well as high risk payments such as payments to one-time vendor accounts. The following reports are generated by the payment program:

- 'Payment proposal list’ - lists all payment line items by business area, payment method and bank;
- 'Payment exceptions list’ - lists all accounts or line items that are blocked for payment. Also lists any other open items that have not been ‘proposed’ for payment. This report will also provide details of any lost prompt payment discounts. This report should be reviewed to ensure that any errors are corrected before the payment run is processed; and
- 'Payment list’ - lists all payment details that have been processed by the payment program and should be reviewed before printing the cheques or processing the EFT files for payment.

SECURITY CONSIDERATIONS

- Access to the authorization objects used to maintain house banks (the organisation’s bank accounts) and vendor bank accounts (master data) should be restricted.
- Access to sensitive cheque management functions, including the ability to maintain cheque numbers, release cheque numbers for reuse, void issued cheques and delete cheque information, should be restricted. This is controlled via the authorization object ‘Check management: Action auth for company codes’.
- Appropriate consideration should be given to segregating conflicting duties in the procurement cycle. Refer ’Procurement/purchasing activities’ section for further details.
Financial accounting

SECTION CONTENTS

Financial accounting components covered ................................................................. 71

General ledger master maintenance ............................................................................... 72
  General ledger master overview .............................................................................. 72
  Significant risks ........................................................................................................ 72
  Completeness of data entry and processing ............................................................ 73
  Master data changes are authorised ....................................................................... 74
  Useful reports ........................................................................................................... 75
  Security considerations ......................................................................................... 75

Customer master maintenance ................................................................................... 76
  Customer master overview ..................................................................................... 76
  Significant risks ....................................................................................................... 77
  Configuration 'hot spots' ....................................................................................... 77
  Customer master data is entered and processed completely ................................ 78
  Changes are authorised ......................................................................................... 80
  Useful reports ......................................................................................................... 81
  Security considerations ......................................................................................... 81

General ledger processing ........................................................................................ 82
  General ledger overview ......................................................................................... 82
  Significant risks ....................................................................................................... 83
  Configuration 'hot spots' ....................................................................................... 83
  Journals are authorised ......................................................................................... 84
  Completeness of data entry ................................................................................. 85
  Processing is complete ......................................................................................... 87
  Useful reports ......................................................................................................... 89
  Security considerations ......................................................................................... 91

Asset accounting ...................................................................................................... 92
  Asset overview ....................................................................................................... 92
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset acquisition process</strong></td>
<td>93</td>
</tr>
<tr>
<td>Asset acquisition overview</td>
<td>93</td>
</tr>
<tr>
<td>Significant risks</td>
<td>94</td>
</tr>
<tr>
<td>Configuration 'hot spots'</td>
<td>94</td>
</tr>
<tr>
<td>Asset master records are completely and accurately created</td>
<td>95</td>
</tr>
<tr>
<td>Useful reports</td>
<td>97</td>
</tr>
<tr>
<td>Security considerations</td>
<td>97</td>
</tr>
<tr>
<td><strong>Asset transfer/retirement process</strong></td>
<td>98</td>
</tr>
<tr>
<td>Asset transfer/retirement overview</td>
<td>98</td>
</tr>
<tr>
<td>Significant risks</td>
<td>99</td>
</tr>
<tr>
<td>Configuration 'hot spots'</td>
<td>99</td>
</tr>
<tr>
<td>Asset transfers and retirements are completely and accurately processed</td>
<td>100</td>
</tr>
<tr>
<td>Useful reports</td>
<td>101</td>
</tr>
<tr>
<td>Security considerations</td>
<td>101</td>
</tr>
<tr>
<td><strong>Asset depreciation/periodic processing</strong></td>
<td>102</td>
</tr>
<tr>
<td>Asset depreciation overview</td>
<td>102</td>
</tr>
<tr>
<td>Significant risks</td>
<td>103</td>
</tr>
<tr>
<td>Configuration 'hot spots'</td>
<td>103</td>
</tr>
<tr>
<td>Depreciation postings are completely and accurately processed</td>
<td>104</td>
</tr>
<tr>
<td>Useful reports</td>
<td>105</td>
</tr>
<tr>
<td>Security considerations</td>
<td>105</td>
</tr>
</tbody>
</table>
Financial accounting

The financial accounting module (FI) consists of several components including general ledger, accounts receivable, accounts payable, assets accounting, legal consolidation, and special ledger. Special ledger is a reporting system that can be used to combine and summarise information from several SAP modules for reporting purposes. Legal consolidation is used to consolidate separate entities. This section of the handbook covers general ledger, accounts receivable and assets accounting. Accounts payable has been addressed in the 'Procurement to payables' section of the handbook.
General ledger master overview

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.

**SIGNIFICANT RISKS**

- Unauthorised users have the ability to make changes to the chart of accounts.
Completeness of data entry and processing

General ledger master data may not be entered or processed completely, resulting in invalid data in the chart of accounts.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that master data is entered and processed accurately and completely:

- The chart of accounts can be configured to ensure that the creation and use of general ledger accounts is controlled. It is possible to define the field status groups and account groups for general ledger accounts, the currency, whether accounts are balance sheet or profit and loss, whether the account is to be used as a reconciliation account, and whether the account can only be posted to automatically. These settings should be appropriately configured for each different account.
- General ledger accounts not assigned to a specific position within the financial statements are highlighted as ‘accounts not assigned’ when the financial statements are produced.
- The profit or loss in the financial statements is calculated by totalling all the accounts that are not assigned or allocated to asset or liability items.
- General ledger account types are assigned to a specific position within the financial statements.
- Accounts that are to be created as reconciliation accounts should be prevented from manual postings to ensure that the control account and subledger remain in balance.

**Desirable**

- The standard audit trail report for changes to general ledger master records can be reviewed on a regular basis to ensure that all changes are authorised.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that master data is entered and processed accurately and completely:

- The system checks for duplicate general ledger account numbers when new master records are created.
- Every master record must be assigned to an account group. The account group controls the numbering for each type of master record based on an internally or externally assigned number range and the fields that will appear when creating a new general ledger account. It also controls the field status settings.
- G/L master records can be created using sample accounts. The system enters default data in the company code-specific fields. Data transfer rules then determine which fields will be transferred when creating a new G/L account and whether a field can be changed.
- Configuration of a general ledger account is maintained at the chart of accounts level and the company code level.
Master data changes are authorised

Changes to general ledger master data may not be authorised, resulting in errors or inappropriate changes remaining undetected.

**BEST PRACTICE PROCEDURE**

*Best practice procedures which could be implemented to ensure that changes to master data are appropriately authorised:*

**Critical**

- Changes to general ledger master data should be appropriately restricted via well defined authorisation controls. Refer to 'Security considerations' on page 75.

**Important**

- The log of document changes should be reviewed on a regular basis by an appropriate level of management. Refer 'Useful reports' on page 75.
- Changes made to general ledger accounts should only be on the basis of an amendment form which has been approved by an appropriate official.

**STANDARD FEATURES**

*SAP also has some standard features which help to ensure that changes to master data are appropriately authorised:*

- The system retains an audit trail for all changes made to general ledger master data and documents. These can be reviewed at any time to determine whether unauthorised changes have been made.
USEFUL REPORTS

Audit trails of changes made to financial accounting master data can be regularly reviewed to ensure that changes are appropriate. These can be accessed via the standard reporting tree and the following reports are available:

- 'General ledger account changes' - provides details of all fields that have been changed for the selected general ledger account. It is possible to drill down to display details of the user who performed the change and the time and date of the change;
- 'Customer changes (accounting)' - similar report providing details of changes to customer accounting related data; and
- 'Vendor changes (accounting)' - similar report providing details of changes to vendor accounting related data.

SECURITY CONSIDERATIONS

- The ability to create, change, delete and block/unblock general ledger master records should be restricted using the authorisation objects 'G/L Account: Authorization for charts of accounts/company codes'.
- Using the optional authorisation object 'G/L Account: Account authorization' it is possible to restrict the range of general ledger accounts that a user can maintain. Consideration should be given to using this object.
- The functions of creating and maintaining FI master data records (banks, G/L accounts, accounts receivable and accounts payable) should be segregated from:
  - creating and posting general ledger transactions; and
  - maintaining the chart of accounts and financial statement(s) structures.
Customer master maintenance

Maintenance of customer master data involves creating and changing customer master records. If the sales and distribution module is implemented, customer master records should be created centrally to ensure that all sales as well as accounting data is maintained.

Customer master records can be maintained via two methods in the SAP system. If the sales and distribution module has been implemented, master records are generally maintained centrally, which allows maintenance of all customer master data views including the sales and accounting information. Alternatively, customer master records can be maintained in the financial accounting accounts receivable module where only general and accounting data can be maintained. It is this process that is addressed in this handbook (the sales and distribution module is not within the scope of the handbook).
SIGNIFICANT RISKS

- All of the data required to create/maintain a complete customer master record (e.g., sales data) may not be entered for processing.
- Duplicate customer master records may be created.
- Unauthorised changes may be made to customer master records.

CONFIGURATION ‘HOT SPOTS’

- The error message for highlighting potential creation of duplicate customers should be activated via message control.
- Data entry characteristics should be appropriately defined to ensure that all fields required during data entry are set to ‘required entry’.
Customer master data is entered and processed completely

Customer master data may not be entered completely, resulting in incorrect customer master details on the system.

**BEST PRACTICE PROCEDURE**

**Critical**

- Key customer master record fields should be defined as ‘required entry’ to ensure that all data necessary to the successful maintenance of a customer master record is entered for processing. Key fields which are not set as ‘required entry’ by default include:
  - payment terms;
  - currency; and
  - exchange rate type.

If the sale and distribution module is being used, the following fields should also be defined as ‘required entry’:

  - customer pricing procedure - note that pricing fields should be ‘required entry’ if prices are to be automatically determined for customers and/or materials; and
  - price list type.

**Important**

- The system can be configured to check for duplicate records when creating customers and vendors. A message appears that the address is the same, and the user should check for a duplicate. A list of potential duplicates appears, and the user can display the individual records to check for actual duplicates. This message should be activated for online entry.

- Postings in the sub-ledgers (FI accounts payable and FI accounts receivable) result in an automatic update to the appropriate reconciliation accounts in the general ledger on a real time basis. For this to occur, each vendor/customer must be assigned to a reconciliation account within the general ledger. The reconciliation account should be set as a ‘required entry’ field as noted above.

- The standard audit trail report for changes to customer master records should be reviewed on a regular basis to ensure that all changes are accurately processed.

**Desirable**

- Procedures should be implemented to ensure that all the necessary customer master details are maintained.
SAP also has some standard features which help to ensure that customer master data is processed completely and accurately:

- Every customer master record must be assigned to an account group which determines the number range for customer master records and the fields that will appear on the screen when creating a customer. It also controls the field status for customer master records.
### Changes are authorised

Changes to customer data are processed without authorisation resulting in unauthorised or fraudulent customer data on the system.

#### Best practice procedure

Best practice procedures which could be implemented to ensure that changes to customer data are authorised:

- Access to customer master maintenance should be restricted. Refer to 'Security considerations' on page 81.

#### Standard features

SAP also has some standard features which help to ensure that changes to customer data are authorised:

- All changes to customer master data can be reviewed via the standard audit trails provided online. Refer 'Useful reports' page 81.
USEFUL REPORTS

- The ‘Master data comparison’ report should be run on a regular basis to ensure that any customer master records maintained without the appropriate sales data are corrected.

- ‘Display of customer changes’ - provides details of all fields that have been changed for the selected customer account. It is possible to drill down to display details of the user who performed the change and the time and date of the change. Note that similar reports are available for the sales and accounting functions. A central report can also be reviewed to provide information on all master data views. This report should be used if customers are maintained centrally.

- The report ‘Customer list’ can be used to produce a list of financial-accounting-related data for selected customer master records. The information reported may include address data, account and control status, tax information (if applicable), bank and payment data, credit limit data and other information.

- There are several credit management reports that should be reviewed on a regular basis to assist in managing customer credit limits if this control feature has been implemented:
  - ‘Customers with missing credit data’ - this report checks the credit limit data in the selected customer master records and determines whether the credit management information is complete. Any omissions are reported and should be followed up and appropriate corrective action taken; and
  - ‘Credit management change display’ - this report provides a list of changes that have been made to the selected master data. It is possible to report on all changes for a particular company code which allows an independent review of credit limit changes.

SECURITY CONSIDERATIONS

- The functions of creating and maintaining customer master records should be segregated from other functions in the system, including posting customer invoices and processing customer receipts.

- Consideration should be given to restricting the range of customer accounts that a user can maintain using the optional authorization object ‘Customer: Account authorization’.

- It is possible to restrict user access to process master data for sales or accounting using the authorization object ‘Customer: Application authorization’.

- The ability to change a customer’s account group can be restricted via the authorization object ‘Customer: Change authorization for account groups’.

- Consideration should also be given to protecting groups of fields from maintenance using the optional authorization object ‘Customer: Change authorization for certain fields’.
General ledger processing

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 (e.g., acquisition of assets, purchases, sales) also result in a real-time update of the relevant accounts in the general ledger.

Customer invoices can be processed via two methods in the SAP system. If the sales and distribution module has been implemented, invoices are produced as part of the billing function, which follows from the process of processing a sales order and despatching goods to a customer. The invoice automatically updates the general ledger in financial accounting. Alternatively, invoices can be processed directly via the financial accounting accounts receivable function. It is this process that is addressed in this handbook.

The better practices identified in the following tables relate to both the general ledger and accounts receivable modules. Some procedures specific to accounts receivable have also been discussed.
SIGNIFICANT RISKS

- General ledger documents may be processed without appropriate authorisation or review by management.
- Unauthorised recurring entry documents may be created for regular processing in the system or changes may be made to recurring entry reference documents without appropriate review.
- Documents may be posted to past or future accounting periods.
- Users have the ability to change documents after they have been posted.
- Duplicate accounts receivable invoices may be processed.

CONFIGURATION ‘HOT SPOTS’

- Consideration should be given to developing additional validation checks to ensure that only valid combinations of data are entered for processing.
- Document change rules should not be modified from the standard settings to ensure that the integrity of transaction data is not compromised.
Journals are authorised

Unauthorized general ledger journals may be processed resulting in postings that are incorrect or fraudulent.

**BEST PRACTICE PROCEDURE**  
Best practice procedures which could be implemented to ensure that general ledger journals are appropriately authorised:

**Critical**

- Access to journal processing (general ledger functions) should be restricted. Refer to 'Security considerations' on page 91.
- General ledger balances should be reviewed and reconciled on a monthly basis. This should be performed as part of month-end processing to ensure that only authorised journals have been processed. The standard reports available in SAP can be used to assist in this process. Refer to 'Useful reports' on page 89.

**Important**

- A pre-input review may also be performed to ensure that only authorised journals are entered for processing.

  If stronger authorisation controls are required, consideration should be given to using the ‘park and post’ functionality. This enables a separation of document entry (parking the document) and posting the document, which effectively acts as an electronic authorisation of the transaction.

- Changes made to automatic postings (refer further detail below) should be authorised by management. A periodic review of automatic postings should be performed to ensure they are appropriate.

**STANDARD FEATURES**  
SAP also has some standard features which help to ensure that all journals are authorised prior to data entry:

- Parked documents do not update any transactions within the system until they are released/posted.
- SAP performs the necessary automatic calculations (such as tax charges, discounts and exchange differences) for parked documents.
Completeness of data entry

All required data for processing general ledger journals is not entered accurately and completely, resulting in erroneous postings.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that all journals are entered for processing accurately and completely:

**Critical**

- Recurring entry original documents should be reviewed prior to posting to ensure that the values to be posted are appropriate. These should be updated whenever necessary.
- General ledger balances should be reviewed and reconciled on a monthly basis. This should be performed as part of month-end processing to ensure that all journals have been processed completely. The standard reports available in SAP can be used to assist in this process. Refer to ‘Useful reports’ on page 89.

**Important**

- A pre-input review may also be performed to ensure that only authorised journals are entered for processing.

  Consideration may be given to using the ‘park and post’ functionality as an alternative means of providing a check on the completeness of data entry. This enables a separation of document entry (parking the document) and posting the document, which effectively acts as an electronic authorisation of the transaction.
- Any outstanding parked documents on the system should be identified and followed up using the appropriate reports. Refer to ‘Useful reports’ on page 89.
- Held documents stored on the system should be identified and followed up. A held document does not update any account balances and can only be further processed by the user who initiated the transaction. As a result held documents are difficult to monitor in the system and procedural controls should be implemented to ensure that held documents are followed up on a regular basis.
SAP also has some standard features which help to ensure that all journals are completely and accurately entered:

- General ledger journals entered into the SAP system consist of a document header and at least two detailed line items. The following fields are compulsory:
  
  **Document header:**
  - transaction date;
  - posting date;
  - document date;
  - document type;
  - company code; and
  - currency.

  **Line items:**
  - posting key;
  - account number; and
  - amount.

- Data entered into fields is checked against data held in master files, including the:
  - accounting data (account name and type, posting types etc);
  - material data (material name and measure, delivery tolerances, prices etc);
  - vendor data (vendor details including payment terms and delivery); and
  - customer data (customer details, including credit limits).

- SAP performs online edit and validation checks against data entered. The user is immediately notified of any errors through the error message on the screen. These must be corrected and resubmitted prior to further processing.

- If a posting date is not supplied for a reversing entry, the system defaults the posting date of the document being reversed. If this accounting period is no longer open, the user must open it or specify another period for reversing the document.

- Documents can only be reversed if:
  - the document has no cleared items;
  - the document has only vendor, customer or general ledger items;
  - all specific values (such as cost centre) are still valid; and
  - the document was posted within the FI System (not SD or MM).

- Reversing documents are subject to the same edit and validation controls as other manual postings.

- Parked or held documents do not result in the update of any data on the system.

- The system records all changes to master records and documents.

- SAP can record data entry control totals for each user, including:
  - the number of documents entered;
  - total debits and credits per G/L, A/R and A/P; and
  - totals of debits and credits per user defined account.

- Transactions entered via a batch interface or processed as recurring journals are subject to the same edit and validation checks as journals processed online in the system.
Processing is complete

General ledger journals may not be completely processed, resulting in data being omitted from the financial accounts.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that general ledger processing is performed completely and the financial accounts updated:

**Critical**

- Posting periods can be created and either opened or closed to document posting. It is also possible to restrict the type of account to which documents may be posted. Only the current posting period should be open for posting.
- General ledger balances should be reviewed and reconciled on a monthly basis. This should be performed as part of month-end processing to ensure that all journals have been processed completely. The standard reports available in SAP can be used to assist in this process. Refer to ‘Useful reports’ on page 89.
- A document can be displayed or changed at any time. It is possible to determine which document fields are allowed to be changed and under what circumstances. Sensitive fields should be prevented from being changed.

**Important**

- A custom report should be developed to ensure that potential duplicate accounts receivable invoices are identified and followed up on a timely basis. This does not apply to sales and distribution billing documents as these are automatically converted to invoices.
- Procedures should be implemented to ensure that the accounting period is closed for posting a pre-defined number of days after period end.
- Comprehensive day, month and year-end processing procedures should be defined to ensure that no critical processing steps are omitted. A checklist should be developed to assist with this process. Period-end processing procedures should include the running of key reports to monitor transactions processed, as well as the posting of accrual and depreciation entries. Refer to ‘Useful reports’ on page 89 for further details of suggested period end procedures.
- Automatic postings can be defined within the system and will ensure that the appropriate general ledger accounts are automatically updated upon processing of defined transactions in the system. Automatic postings should be appropriately configured.
- Each general ledger account type should be assigned to a specific position within the financial statements. This classification should be reviewed and approved by senior finance management.
- On a periodic basis (e.g. 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.
• Consideration may be given to the use of custom validations to ensure that only valid combinations of accounts are processed (e.g., check that the general ledger account can be posted to, for the selected cost or profit centre).

• Various tolerances and settings can be defined for customers to control clearing (payment) procedures, set limits for payment differences, specify how residual payment items (under- or over-payments) are to be treated, and set tolerance limits for the creation of residual items. These settings should be appropriately configured.

• Year-end closing procedures should be developed. The appropriate posting periods should be closed and the month-end closing procedures performed.

**Desirable**

• If a transaction is posted to an account that is marked for deletion, a warning message is provided for the user, although this can be ignored and the transaction posted. Procedures should be implemented to ensure that accounts marked for deletion are also blocked for posting.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that general ledger processing is performed completely and the financial accounts updated:

• If a transaction is posted to an account that is blocked for posting, an error message is generated. Blocking a master record prevents posting to a general ledger account, vendor or customer, and can affect other module activities (such as creating sales orders in sales and distribution).

• General ledger postings must balance to zero (debits must equal credits) before the document can be processed.

• Accounting related data (account number, amount and posting key) cannot be changed once a document is posted.

• The document reversal function automatically reverses an entry (so that all the original information and accounts are intact) and creates a new document with reference to the original posting.

• Recurring journal automatic batch runs result in the creation of an accounting document and updates to the original recurring entry document and the next run date.
USEFUL REPORTS

- There are a number of standard system reports that can be reviewed on a regular basis to ensure that postings to the financial accounts are appropriate. These reports are available via the standard reporting tree, menu path: Accounting ➔ Financial accounting ➔ General ledger ➔ Periodic processing ➔ Info system ➔ Report selection... . The following reports should be regularly reviewed:
  - ‘Compact document journal’ - this report details all transactions processed in the system and allows selection according to a range of detailed criteria for several document types, including standard documents, parked documents, and recurring documents. This report also allows the use of ‘dynamic reporting’ for more flexible reporting;
  - ‘General ledger account balances’ - provides a summary of all transactions processed through the general ledger. The debit and credit totals from this report should reconcile to the totals from the Compact document journal. This report also allows the use of ‘dynamic reporting’ for more flexible reporting;
  - ‘Customer account balances’ - provides a list of all transactions processed against the selected customer accounts (control accounts) in the general ledger. The totals from this report should reconcile to the Compact document journal and the balances for the control accounts in the general ledger account balances report. This report also allows the use of ‘dynamic reporting’ for more flexible reporting;
  - ‘Vendor account balances’ - provides a list of all transactions processed against the selected vendor accounts (control accounts) in the general ledger. The totals from this report should reconcile to the Compact document journal and the balances for the control accounts in the general ledger account balances report. This report also allows the use of ‘dynamic reporting’ for more flexible reporting; and
  - ‘FI document: List of update terminations’ - this report provides a list of any unposted documents and should be run weekly to ensure that all documents have been completely posted.

- Appropriate period-end closing procedures should be defined in detail to ensure that users are able to perform all period end activities completely. Procedures should be defined for month-end and year-end processing to ensure the financial accounts are completely and accurately updated and should include (but not be limited to) running the following reports:

  **Month-end closing:**
  - ‘Compact document journal’ (as discussed above);
  - ‘Posting totals’ - provides a summary of all debit and credit postings by company code, business area, document type and separated by account type;
  - ‘Revalue open accounts’ - used to revalue any unpaid invoices valued in foreign currencies;
- ‘Balance sheet supplement-open item analysis’ - provides an analysis of open receivables and payables balances and posts any adjustments necessary. This report is also used to reclassify receivables with credit balances and payables with debit balances;
- ‘Document reconciliations’ - compares transaction totals from vendor and customer accounts with transaction totals from documents posted in the period to ensure they reconcile; and
- Run monthly financial statements. Any variances highlighted should be fully investigated and corrections made as necessary.

A regular review should be performed for recurring documents that are processed on the system, to ensure that the amounts to be posted are appropriate. The following reports should be regularly reviewed:

- ‘Recurring entry documents’ - provides a list of the selected recurring entry documents. A review of recurring entry documents that are about to expire may be useful to assess whether these documents should be renewed; and
- The ‘Display of changed documents’ report should be reviewed on a regular basis to identify any changes to recurring entry original documents and other document types (including parked and sample documents). This should be reviewed by management independent of the process, to ensure the changes are authorised and appropriate.
SECURITY CONSIDERATIONS

**General ledger**

- 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 authorization object ‘Accounting document: Authorization for account types’.

- 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.

- Access to work with the financial statements should be restricted from users who have access for general ledger transaction processing. This is controlled via the authorization object ‘Balance sheet: General maintenance authorization’.

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

- 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.

- Limits can be defined to limit the amounts that users can post 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.

**Accounts receivable**

- The invoice processing function should be appropriately segregated from functions such as credit control, general ledger posting, delivery of goods, cash receipting, and maintenance of customer master data.

- Consideration should be given to restricting access to post invoices by company code, business area, document type and account type.

- Access to post invoices can be restricted by customer account type using the optional authorization object ‘Accounting document: Account authorization for customers’.
The SAP asset accounting module is a sub-module of the financial accounting module. It allows an organisation to record and manage its fixed asset resources. The asset accounting module is used for processing the acquisition, transfer, retirement and depreciation of fixed assets.
An asset master record must be created before a purchase order for the asset can be raised. The asset master record contains all the critical information which is stored in the system relating to an asset. The asset acquisition process is largely dependent on the materials management purchasing process. Refer to ‘Procurement to payables’ section. Asset acquisitions can also be processed via manual journals raised in the financial accounting module or via a settlement made through the project systems module.
SIGNIFICANT RISKS

- The asset master record may not be set up correctly, or may not contain all of the necessary data.
- If documented procedures are not in place for processes such as the acquisition, maintenance, transfer and retirement of fixed assets, then these processes may be performed inconsistently or incorrectly.
- Upon creation, assets could be allocated to the incorrect asset class. This may result in, amongst other things, the incorrect depreciation treatment.
- Low value assets (LVAs) could be incorrectly classified. The maximum LVA amount could be set in the system inconsistently with the agency’s LVA policy.

CONFIGURATION ‘HOT SPOTS’

- Field status settings should be set to reflect whether the various fields on the asset master record should be ‘required’, ‘display only’ or ‘suppressed’.
- Some screens may exist on the asset master records which do not require processing. If not suppressed, these may cause confusion if users do not know to bypass them.
- Asset classes should be configured appropriately so that the correct default values, such as depreciation keys, are used when asset master records are created.
- Ensure correct nomination of the general ledger accounts to which asset acquisitions are posted.
Asset master records are completely and accurately created

Failure to create asset master records completely and accurately could result in an inaccurate fixed assets register and, consequently, poor control over assets or unreliable financial reporting.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that asset master records are completely and accurately created:

**Critical**

- 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 (e.g., asset class, company code, description). Additional fields which should be set as ‘required entry’ include:
  - business area (if used);
  - cost centre;
  - plant; and
  - location.

- Asset classes which are required should be identified and configured appropriately. Control parameters and default values for the various classes should be considered and defined. For example, the depreciation key should default for an asset class so that all assets within that class are depreciated consistently.

- 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.

**Important**

- 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 and processed completely and accurately.

- Assets should be periodically verified via a physical count.

- 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.

- 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 LVA’s.
Security and Control for SAP R/3 Handbook

Desirable

- The maximum LVA amount should be set in SAP in accordance with the agency's LVA policy.
- Internal asset number assignment is considered to be best practice. Although there is protection against duplicate asset numbers with external number assignment, internal number assignment ensures a consistent approach to the numbering of assets.
- Redundant screens on the asset master record should be suppressed to prevent user confusion and increase the efficiency of assets processing.

STANDARD FEATURES

SAP also has some standard features which help to ensure that all asset master records are accurately and completely created:

- Each asset must belong to an ‘asset class’ (refer glossary at Appendix 2). Asset classes can be set up to provide automatic values which will be applied consistently across the asset class. Screen layout and field status settings can be defined for an entire asset class which control the inclusion/exclusion of data entry into certain fields. Asset classes can also be used to determine which general ledger accounts are posted to for an asset transaction. Default values can be set up for asset classes and these are particularly useful for fields such as ‘depreciation key’, as all assets within a class should be depreciated in a like manner.
- Key fields (e.g., company code) will be automatically checked by SAP before the system will allow the user to save an asset master record. Mandatory fields (e.g., description) will also be required to have data entered before SAP will allow the record to be saved.
- Each asset is assigned a unique asset number. The asset number may be internally (system generated) or externally (user entered) assigned. If externally assigned, SAP will issue an error message if a duplicate asset number is entered.
- When the goods receipt or invoice receipt is processed, the costs associated with the purchase of the asset are automatically capitalised. The system determines which asset to post costs against via the account assignment data that was entered on the purchase order. This ensures that, providing the procedure has been followed properly, all assets will be capitalised.
USEFUL REPORTS

Several reports are available to assist in monitoring fixed assets acquisitions and can be found in the asset accounting information system (Accounting ➔ Financial Accounting ➔ Fixed assets ➔ Info system ➔ Report selection). The following reports should be regularly reviewed:

- The ‘Asset acquisition’ report should be periodically reviewed to ensure that all assets entered into the system have been authorised.
- The ‘Directory of unposted assets’ report should be periodically reviewed to ensure that there are no assets not yet capitalised which should have been.
- The ‘Changes to asset master records’ report should also be periodically reviewed to ensure that all changes made to asset master records were authorised and accurately processed in the system.

SECURITY CONSIDERATIONS

- Consideration should be given to segregating asset accounting processing from the procurement and general ledger functions.
Asset transfer/retirement process

Asset transfers may be performed on an intra-company (within the same company code) or inter-company (between company codes) basis. A number of options exist for asset retirements such as scrapping or sale with or without a customer.
**SIGNIFICANT RISKS**

- Assets are transferred to the wrong location, or the wrong assets retired due to the system being incorrectly set up.
- Failure to process asset transfers or retirements altogether. This will result in an inaccurate fixed assets register and incorrect financial statements.

**CONFIGURATION ‘HOT SPOTS’**

- Ensure correct nomination of the general ledger accounts to which asset retirements and transfers are posted.
- Care should be taken to ensure settings for asset transfer and retirement transaction types are appropriate.
Asset transfers and retirements are completely and accurately processed

Failure to process asset transfers and retirements completely and accurately could result in an inaccurate fixed assets register and a loss of control over fixed assets.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that asset transfers and retirements are accurately and completely processed:

- **Critical**

  - Asset transfer and retirement transaction types should be set up to ensure that the correct result is obtained when the transaction is posted. If new transaction types are defined they should use the standard SAP naming conventions.

- **Important**

  - 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.

  - 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.

  - 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.

  - Assets should be periodically verified via a physical count.

- **STANDARD FEATURES**

  - SAP also has some standard features which help to ensure that asset transfers and retirements are accurately and completely processed:

    - Asset transfers and retirements are performed using a transaction type which is simply a code used to identify the business transaction. Asset transfer transaction types are in the range 300-399, while asset retirement transaction types are in the range 200-299. Transaction types are set up to control such parameters as account assignment, depreciation treatment and the timing of the transfer/retirement.

    - Date specifications are required by SAP to determine the document date (issue date of the original document) and the posting date (date transaction is posted to the G/L) of the transfer/retirement. SAP will automatically check that the dates are acceptable and in the correct date format.
• Key fields (eg asset number) will be automatically checked by SAP before the system will allow the user to post an asset transaction. Mandatory fields (eg transaction type) are also required to be populated before SAP will allow the transaction to be posted.

• A document which is assigned a unique document number is generated by the system which records all the details of the asset transfer/retirement. These documents may be viewed online.

• On transfer or retirement of an asset, the accounting entries required, such as profit or loss on the transaction, are automatically calculated by SAP, based on master data and account assignments.

**USEFUL REPORTS**

Several reports are available to assist in monitoring fixed asset transfers and retirements. These can be found in the asset accounting information system (Accounting ➔ Financial accounting ➔ Fixed assets ➔ Info system ➔ Report selection). The following reports should be regularly reviewed:

- The ‘Asset transfers’ report should be periodically reviewed to ensure that all asset transfers have been authorised and accurately processed in the system.
- The ‘Asset retirements’ report should be periodically reviewed to ensure that all asset retirements have been authorised and accurately processed in the system.

**SECURITY CONSIDERATIONS**

- Consideration should be given to segregating asset accounting processing from the procurement and general ledger functions.
Asset depreciation/periodic processing

Depreciation is usually posted to the general ledger in SAP on a monthly basis. Depreciation is posted by creating a batch job and processing this in the background. The actual depreciation posted is calculated according to the depreciation key which is stored on each asset master record. Separate asset ledgers can also be kept for other purposes such as tax and historical cost ledgers.
**SIGNIFICANT RISKS**

- Incorrect depreciation may be posted if master records are not set up with the appropriate depreciation keys.
- If asset posting periods are not strictly controlled depreciation expenses could be posted to the incorrect accounting period.

**CONFIGURATION ‘HOT SPOTS’**

- The formula in a calculation key must correspond to the depreciation key.
- Ensure correct nomination of the general ledger accounts to which depreciation entries are posted.
- Asset classes should be configured appropriately so that default values for depreciation keys are used when asset master records are created.
- Depreciation areas should be configured appropriately, including the prevention of negative book value.
Depreciation postings are completely and accurately processed

Failure to process depreciation postings completely and accurately could result in costs being allocated incorrectly or not recorded at all.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that depreciation postings are completely and accurately processed:

**Critical**

- Depreciation keys are the link between the asset master record and the calculation key. The calculation key is where the formula for the calculation of the depreciation is set up. The calculation performed by the calculation key should reflect its description and the description of the depreciation key that it is linked to.
- 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.
- The calculation key should be configured to calculate depreciation from the correct asset value; i.e., it should usually perform the calculation based on the assets acquisition value, not on its replacement value or any other value.

**Important**

- The depreciation keys for each depreciation area and the asset's useful life should be defaulted. This is dependent upon the asset class.
- 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.
- Depreciation areas should be configured appropriately, including the prevention of negative book value.
- Key staff members should be provided with adequate training to ensure that maintenance of standing data (such as depreciation keys and asset classes) is completely and accurately performed.
- 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.
- Cost centre owners should periodically review reports of the assets which belong to their cost centres to ensure that depreciation charges are reasonable.
SAP also has some standard features which help to ensure that depreciation postings are accurately and completely processed:

- Asset master records can have one or many depreciation areas defined. For most departments, only depreciation area 01 (book depreciation) is required. However for tax-paying agencies, depreciation area 15 (tax balance sheet) will also be required to keep track of tax depreciation values.

- Key fields (eg company code, posting period) will be automatically checked by SAP before the system will allow the user to create the depreciation batch session. Mandatory fields (eg session name) are also required to be populated before SAP will allow the session to be created.

- A batch session is created which will post the depreciation. The batch session can only be run once and will not post transactions which contain errors. If the posting does not work the batch session can be recreated.

- When the depreciation batch session is processed, the accounting entries required are automatically calculated by SAP based on master data and account assignments.

USEFUL REPORTS

Several reports are available to assist in monitoring the posting of depreciation. These can be found in the asset accounting information system (Accounting ➔ Financial accounting ➔ Fixed assets ➔ Info system ➔ Report selection). The main report which should be periodically reviewed is:

- The ‘Depreciation’ report to ensure that depreciation postings have been accurately and completely processed in the system.

SECURITY CONSIDERATIONS

- Consideration should be given to segregating the processing of asset accounting from the procurement and general ledger functions.
Controlling

SECTION CONTENTS

Controlling overview ................................................................. 108
Cost allocations and transaction postings .................................... 109
Significant risks ........................................................................ 110
Configuration ‘hot spots’ ............................................................. 110
Postings are processed completely and accurately ..................... 111
Useful reports .......................................................................... 113
Security considerations ............................................................... 113
Controlling

Controlling overview

The controlling module (CO) is primarily used for management reporting purposes. It is a central function within the SAP system which is used for reporting on revenue and expense items only. The CO module consists of the following modules:

- **CO-CCA cost centre accounting**: the cost centre accounting functionality of the CO module allows costs to be allocated to cost centres, then to be distributed either by reallocation of costs directly, or by allocating costs from cost centre to cost centre on the basis of activities performed. This is a complex module which can be used for reporting, planning and budgeting;

- **CO-ABC activity based costing**: activity based costing allows additional capabilities for allocating costs to products based on the processes performed by the organisation;

- **CO-OPA order and project accounting**: OPA allows grouping of costs by internal orders and projects. Costs are grouped by internal orders based on the time or reason that they were (or will be) incurred. Projects are a more formal method of grouping costs and are used for creating assets that will be capitalised or included in inventory;

- **CO-PC product costing**: product costing and base object costing can be used as another means of estimating the cost of the product being manufactured;

- **CO-PA profitability analysis**: PA is used to calculate operating profit and contribution margins for management analysis; and

- **CO-PCA profit centre accounting**: PCA is used to determine internal profit and loss analyses for profit centres. This makes it possible to evaluate different areas or units within the organisation which operate independently.

The controlling module is interfaced with other modules in the SAP system via a central interface. Postings performed in other modules (e.g., general ledger) will automatically update the controlling module on a real-time basis provided the relevant information is entered as part of data processing in the originating transaction.
Cost allocations and transaction postings

It is the CO-CCA cost centre accounting module which is covered in this handbook. It is considered that this functionality of the CO module is the most commonly used across the various organisations that implement SAP within the Commonwealth.
SIGNIFICANT RISKS

• Transaction postings in SAP application modules (e.g., FI, MM, FI-AA) may not update the controlling module if the central interface is not appropriately configured.

CONFIGURATION ‘HOT SPOTS’

• Ensure that the appropriate accounts are defined for the FI-CO reconciliation posting.
• Control indicators should be appropriately set for each controlling area to ensure that the relevant controlling module components are activated.
Postings are processed completely and accurately

Postings may not be processed completely, resulting in errors in the accumulation and reporting of costs.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that postings to the controlling module are performed accurately and completely:

**Critical**

- It is possible to activate or deactivate the SAP modules that can interface with the CO module. All modules that are required to update CO postings should be activated for the current fiscal year.

**Important**

- 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.

- Clearing accounts should be defined for company code and business area clearing to ensure that the system can generate the appropriate FI document to complete the reconciliation.

- 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.

- Transactions that are always posted to the same cost centre, profit centre or order, should be set up to ensure that these postings are automatically performed by the system using automatic account assignments.

- Code combinations should be used to ensure that the ability to perform cost centre postings is restricted to the appropriate company codes or business areas.

- Control indicators should be appropriately configured for each controlling area to ensure that all controlling components that are intended to be used are activated.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that postings to the controlling module are performed accurately and completely:

- SAP automatically logs all changes that are performed to master records including cost centres, cost elements and activity types.

- Controlling documents can only be created, displayed or reversed but cannot be deleted. This ensures that an audit trail is maintained for all transactions processed on the system.

- The results of all cost postings are stored in ‘line item tables’ in the system. This includes primary and secondary postings. This information is also summarised in ‘totals tables’.
• Journals can only be posted to open accounting periods. Journals are posted on a real-time basis.

• A central interface controls real-time postings to the CO module from other SAP application modules. The system checks the validity of the postings and automatically updates transaction data.

• Costs posted against primary cost elements are directly posted against the financial accounting (FI) profit and loss accounts as well as the appropriate cost centre. In order to create a primary cost element it must also have a corresponding general ledger account in the chart of accounts and it must be defined as an account in the FI module.

• If costs are ‘reposted’ between company codes the FI/CO reconciliation ledger automatically creates a credit entry for the originating company code and a debit entry for the receiving company code.

• SAP performs online edit and validation checks for all data entered. Any errors are highlighted to the user and must be corrected before the document can be posted.

• Cost postings must pass the edit and validation checks of the sending SAP module before they can be interfaced to cost centre accounting (CO).

• The system requires certain information to be entered when creating master records in the CO module.

• The system automatically checks for duplicate master records when a new master record is created.
USEFUL REPORTS

- Various change document reports are available to provide information on changes made to master data elements. The change document reports can be executed via the SAP menus and should be reviewed regularly to assess the appropriateness of changes made to master data.

- Numerous reports are available via the controlling module. Reports detailing costs posted to cost centres/cost elements/orders and other cost collectors should be periodically reviewed by the appropriate level of management to ensure that all cost postings are authorised. Controlling reports can be accessed via the menu path: Accounting ➔ Controlling ➔ Cost elements/Cost centres/Profit centre acctg etc... ➔ Information system ➔ Choose report ...

- The 'Report painter' and 'Report writer' utilities may also be used to assist in developing custom reports for more complex or specialised controlling queries. These utilities were originally developed by SAP to be used in the controlling module.

SECURITY CONSIDERATIONS

- It should be noted that there are limitations in implementing cost centre security for a number of transactions in other modules via the standard security objects. However, there are controlling module authorization objects that can be used to restrict access to cost centres for controlling module transactions.

- Limits can be defined to limit the amounts that users can post 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.
Human resources

SECTION CONTENTS

Human resources overview .................................................. 116
Personnel/human resources functions .................................. 117
  Significant risks .................................................................... 118
  Configuration 'hot spots' ....................................................... 118
  HR master data maintenance is authorised ............................ 119
  HR master data maintenance is entered and processed correctly .................................................. 120
  Useful reports ....................................................................... 123
  Security considerations ....................................................... 124
Payroll calculation and payment ........................................... 125
  Payroll calculation and payment overview ........................... 125
  Significant risks .................................................................... 125
  Configuration 'hot spots' ....................................................... 126
  Payroll data is entered for processing accurately ................ 127
  Gross and net pay are calculated correctly and recorded in the financial accounts ........................................... 128
  Liabilities are correctly calculated and accounted for ........... 131
  Payroll payments are approved ............................................ 133
  Payments are made to the correct employees .................... 134
  Useful reports ....................................................................... 135
  Security considerations ....................................................... 136
Human resources overview

The HR module in SAP is divided into two components - Personnel administration (HR-PA) and Personnel planning and development (HR-PD).

The HR-PA module is used for maintaining employee standing data (e.g., promotions, basic pay information), processing the hiring/termination of employees, processing leave benefits, time management functions, processing of the payroll program, maintenance of travel expenses, administering salaries, and performing recruitment functions. All HR master data is stored in similar groups of information called infotypes.

The HR-PD module is used for administering the organisational structure. It can be used for personnel capacity and cost planning, management of qualifications, training and career/succession planning, as well as organisational planning.

The two components can be implemented separately or may be integrated.
It is the HR-PA module covering the maintenance of employee standing data, processing hiring/terminations of employees, leave benefits and payroll which is primarily covered by this handbook.
SIGNIFICANT RISKS

- Changes to employee data may be performed by overwriting previous data and result in no audit trail being maintained for the changes made.
- Unauthorised users may have access to view/maintain sensitive human resources/payroll data. This may compromise the confidentiality of human resources data and could also result in the processing of fraudulent payroll payments.
- It is possible to change the status of a terminated user to enable payment even after termination.

CONFIGURATION ‘HOT SPOTS’

- Sensitive infotypes should be activated for logging to ensure they are included in the ‘Logged changes in infotype’ audit report.
- The personnel checking function needs to be activated if personnel administrators are to be confined to specific groups of employees.
- HR events should be appropriately configured to include all groups of master data that are required to complete the event/transaction.
- Screen modification rules should be defined to ensure that all key fields are mandatory for data input.
- The appropriate integration switches should be set to ensure that the HR-PA and HR-PD modules are integrated if applicable.
HR master data maintenance is authorised

Changes/additions to HR master data might be performed without appropriate authorisation, resulting in employees being over- or under-paid.

Best practice procedures which could be implemented to ensure that changes to HR master data are authorised:

**Critical**

- Procedural controls should be in place to ensure that changes made to infotypes for HR master data are performed by delimiting (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. The system cannot be configured to enforce users to delimit rather than simply change infotypes.

- Access to perform HR master data maintenance should be restricted to authorised HR staff only. Refer to ‘Security considerations’ on page 124.

**Important**

- It is possible to define an administrator responsible for maintaining particular types of data for specific personnel numbers or groups of personnel numbers. This can effectively be used to segregate HR master data maintenance (eg preventing payroll officers from maintaining their own HR master data). Refer also to ‘Security considerations’ on page 124.

- Specific infotypes can be logged to record changes to the infotype. This log should be activated and then reviewed via the standard report ‘Logged changes in infotype’ to ensure that all changes are authorised.

SAP also has some standard features which help to ensure that changes to HR master data are authorised:

- Changes are performed on HR master data through groups of information called infotypes. Infotypes are created for each master record as applicable and can be maintained.

- SAP will not allow changes to be performed to infotypes 0000 (Events) and 0001 (Organisational assignment) as these are always delimited automatically (that is, a new infotype is created with a new validity date range).
HR master data maintenance is entered and processed correctly

HR master data changes/additions may not be completely entered resulting in HR/payroll data that is incorrect. This could result in employees being over- or under-paid.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that HR master data changes are entered and processed completely:

- Different types of employee master data can be grouped together to create ‘events’. Events can be used to control the information that will be processed when commencing, terminating, and maintaining employee data (e.g., changing basic pay or employee status). 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.

- The ability to change groups of employee master data temporarily should be restricted, especially the removal of infotypes from groups (events).
  
  If this functionality is required, consideration should be given to reviewing the ‘Logged changes in infotype data’ audit report for changes to the ‘Events’ infotype.

- 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 can 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 organisation.

- The ‘double verification principle’ should be considered to ensure that master data changes are completely processed. One user can be assigned the ability to create ‘locked’ HR master data records. A second user is then assigned the authority to ‘unlock’ those records. The second user then performs a check and online authorisation of the first user’s activities.

  An alternative procedure would be to review the audit trail report for changes to HR master data for key master data changes. This procedure should also be supported by the authorisation of all master data amendment forms.

- 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.
Important

- Certain integration switches must be set correctly to ensure that data is transferred accurately and completely between the HR-PA (Personnel administration and payroll accounting) and HR-PD (Personnel planning and development) modules.

- Wage types are defined in the system to assist in the calculation of pay. Wage types can be defined as a payment or deduction and can be configured as an amount or other unit of measurement. Wage types should be appropriately configured to represent the different salaries, allowances, and deductions for the organisation.

- HR master data is defined as being valid for a specified time period. It is possible to define constraints for the time periods that can be used for different types of HR master data. The constraints assigned to each type of master data should be consistent with the purpose of the data (e.g., employee personal details should always exist, even after termination).

- Procedures should be developed to ensure that any master data (infotype) that is not automatically deactivated as part of the ‘termination’ event (e.g., Recurring payments and deductions, additional payments) is deactivated as part of the termination processing. A standard checklist should be developed as part of the termination procedures to ensure that all relevant master data settings are deactivated after termination.

- There is some master data that should not be deactivated even after an employee has been terminated. This includes organisational data, personal data, address data and basic pay data. (e.g., It may be necessary to send information out to a terminated employee. If the deactivated master data has been archived, address details may not be available). Procedures should be developed to ensure that users retain this data on the system for future reference and processing of any subsequent payments.

- The fast entry facility can be used for commencement and some other HR ‘events’. It permits entry of all required data fields. All other fields are automatically filled with default values by the system. All required fields should be defined to ensure that data necessary for the calculation of payroll is not overlooked.

- Appropriate rules should be configured for country specific settings such as bank account numbers and post code data to ensure that this information is completely and accurately entered during master data maintenance.

Desirable

- The system should be configured to assign sequential personnel numbers automatically to new employees.
SAP also has some standard features which help to ensure that HR master data changes are entered and processed completely:

- Delimiting infotypes consists of changing the validity date of the previous infotype and creating a new version of the same infotype with new validity dates. The system prevents overlapping validity dates for the same infotype.

- ‘Features’ control input of certain data in the HR-PA module. For example, features may determine default values for input fields based on settings in certain fields.

- The tracking and collection of organisation assets loaned to employees can be controlled through the ‘Objects on loan’ infotype in the SAP HR-PA module.

- All employee information entered is verified against system tables. The system also proposes default values for many data input fields.

- During data entry key fields are defined as ‘required entry’ by the system. These include the organisation structure fields for the infotype ‘Organisational assignment’.

- When the HR-PA module is integrated with the HR-PD (HR planning) module, the system will automatically default the relevant field values for organisational fields when processing defined ‘events’ (e.g., commencements) based on the ‘position’ entered. Any values overridden by the user will be validated by the system. The relevant switches should be configured to ensure that the PA and PD modules are integrated (if the PD module has been implemented).

- Various organisational criteria can be automatically assigned to an employee via the time, pay scale and wage type structures that are assigned to the employee.

- ‘Employee subgroup’ is used to group employees and control various settings including the basis of payroll calculation, the wage types and pay scale groups applicable for the employee. It also allows default values to be generated for data entry (e.g., payroll accounting area).

- Employee (payroll) status is automatically updated when relevant events are processed (e.g., commencements, termination). The status record is automatically created when an employee commences. The following criteria are controlled by the payroll status:
  - whether the personnel number is locked (excluded from payroll accounting);
  - the last payroll accounting date;
  - the date that the last retroactive calculation was performed;
  - whether retroactive calculations can be performed for the personnel number;
  - the earliest permissible date for a retroactive payroll calculation; and
  - the starting date of the employee’s personal calendar.

- The organisation assignment, personal data, and payroll status infotypes are mandatory and exist from the date of commencing an employee.
USEFUL REPORTS

• The 'Logged changes in infotype data' report should be run on a regular basis to review changes made to key infotypes to ensure they are authorised. This report can be executed via the menu path Human resources ➔ Personnel admin ➔ Info system ➔ Report selection.

   It is possible to display all changes made to an employee file for a specified period. The report displays 'before and after' values for fields groups or infotypes. It is also possible to log changes that have been automatically performed on fields related to the logged field. Individual infotypes that are sensitive in nature should be configured to ensure they can be reviewed using this report.

   It should be noted, however, that this report does not report on just the changed fields for a given infotype. Instead the report will provide details for every field contained within an infotype including fields which have not been changed. As a result the effectiveness of this report is reduced and it may be necessary to consider developing a custom exception report to identify changes to key fields without reporting details of fields which have not changed.

• The report 'Log report starts' can be used to log each time a system report is executed. This report could be used to monitor sensitive HR/payroll reports that are run, as the report details the name as well as the user who executed the system report along with the date/time. The report can be executed via the menu path Human resources ➔ Personnel admin ➔ Info system ➔ Report selection.
SECURITY CONSIDERATIONS

• Access to HR master data is provided through information types called ‘infotypes’. Access to sensitive infotypes (e.g., basic pay, tax file number, personal data) should be adequately restricted to ensure that unauthorised users cannot display or maintain this data. Access can be restricted using the authorization object ‘HR: Master data’.

• The authorization object ‘HR: Master data’ can also be used to implement an online authorisation of HR master data maintenance transactions through the ‘double verification principle’. One user can be assigned the ability to create ‘locked’ HR master data records. A second user is then assigned the authority to ‘unlock’ those records. The second user then performs a check and online authorisation of the first user’s activities.

• Access to table maintenance transactions should be restricted in the system (refer Basis section). Users with access to display/maintain tables may also be able to access sensitive HR data including salary and tax file number data.

• Personnel officers can be restricted to maintain HR master data for a specific group of employees by defining administrators and using the authorization object ‘HR: Master data extended check’. This can effectively be used to segregate HR master data maintenance (e.g., preventing payroll officers from maintaining their own HR master data). The personnel number check must also be activated in the system and employees assigned to administrators.

• Payroll staff should be restricted from maintaining their own HR data including basic pay information. This can be achieved in a number of ways including:
  - activating authorisations based on personnel numbers – it is possible to assign particular users the ability to maintain specific personnel numbers. This can be implemented using the optional authorization object ‘HR: Master data - personnel number check’; or
  - restricting the access of payroll staff to perform only payroll functions while HR staff maintain employee standing data. Changes made by HR employees to their own master data should be logged (using the report ‘Logged changes in infotype’) and approved by an appropriate level of management.

• It is also possible to implement position-based security within SAP. This is considered a best practice approach to implementing security as each employee in the organisation is assigned to a position and the position is then assigned access rights to perform individual tasks in the system. This provides an improved level of control over the updating of access rights when users leave the organisation or transfer to a different position.

• 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.

• ‘PD authority profiles’ can be created to limit an employee’s access to specific PD objects or organisational structures in the HR-PD module, and to control the activities that users can perform for organisational plans in HR-PD. These profiles are provided in addition to the standard authorizations and do not grant but instead limit access. That is, if a user is not allocated a PD authority profile, they would have access to all PD objects (assuming they have the appropriate SAP authorizations).
Payroll calculation and payment

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 organisation.

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 (eg superannuation payments).
SIGNIFICANT RISKS

- Users may have the ability to change the payroll status of an employee, which could result in the employee continuing to be paid after termination.
- The system does not correctly calculate long service leave liabilities per AASB1028/AAS30.
- The payments data file sent to the bank/payment authority with the payroll payment details may not reflect the correct payments to individual employees as processed by the payroll system.

CONFIGURATION ‘HOT SPOTS’

- The earliest dates for which retrospective payroll accounting adjustments can be performed should be appropriately set.
- The payroll period used to create the control records at the productive start of the HR system should be set as the period prior to the first live payroll period.
- The entry of additional wage types via the ‘Employee remuneration information’ screen should be prevented.
- The system should be configured to prevent retrospective payroll adjustments being processed for trivial amounts.
- The default payment method should be set for each payroll accounting area, along with minimum payment amounts and the master file information required to process payroll payments.
- Leave accrual rules should be set up to reflect the relevant awards and maximum accrual amounts and warning messages should be configured where appropriate.
Payroll data is entered for processing accurately

Payroll data may not be entered completely, resulting in payroll calculations that are incorrect.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that payroll data is entered completely and accurately:

**Critical**

- 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 (e.g., this date should not be prior to the system implementation date).

**Important**

- The 'Payroll exceptions report' provides details of any exceptions logged by the system during payroll processing, including any employee master records that contain incomplete information (e.g., 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.

- The payroll period used to create the control records at the productive start of the HR system must be the period prior to the first productive payroll period.

- Each payroll run should be reconciled to the previous period payroll using the standard reports available. Refer to 'Useful reports' on page 135. Payroll totals should also be reviewed by cost centre to ensure that payroll costs are appropriate and have been completely and accurately processed.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that payroll data is entered completely and accurately:

- The system maintains information about the last payroll accounting period for each 'payroll area' in a control record. This information is then used during the next payroll run to determine the dates for the current payroll period.
Gross and net pay are calculated correctly and recorded in the financial accounts

Gross and net pay calculations may not be performed correctly, resulting in incorrect payments of net pay and tax and incorrect recording of payroll expenses.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that gross and net pay are calculated correctly:

**Critical**

- It is possible to enter additional wage types via the infotype 'Employee remuneration information'. This should be restricted to ensure that inappropriate wage types cannot be processed. The system can be configured to specify which wage types can be entered via this screen. The entry of a wage type through 'Employee remuneration information' overrides any existing valuation base for the particular wage type and affects the calculation of employee salary.

- The personnel calculation rules are used in the calculation of gross and net pay for employees and should be protected from being overridden. Changes should be made by making a copy of the original rules and only in the development environment.

**Important**

- The general ledger accounts used for posting payroll expenses and liabilities are defined during configuration. These accounts should be configured appropriately to ensure that the financial accounts accurately reflect the payroll expenses and provisions.

- Wage types should be appropriately configured to ensure that the relevant wage types are included in the calculation of gross pay for an employee. Wage types can be configured as a payment or deduction and for either direct or indirect (system-generated) valuation. Rounding can also be configured.

- Configuration of fields and/or infotypes that can be used to process a retrospective payroll adjustment should be appropriate to ensure that trivial adjustments do not result in a payroll correction being processed.

- 'Check lists' should be created to assist in the reconciliation of the data transfer from the HR module to the FI/CO modules. Totals should be checked by finance staff for the following balances to ensure that the interface has been completely processed and the financial records updated:
  - employee receivables;
  - advance payments;
  - transfers of remuneration; and
  - transfers of capital formation savings payments.

- Superannuation calculation rules should be appropriately configured to ensure the correct calculation of Superannuation Guarantee Charge (SGC) amounts.
• It is not possible to assign a priority to deductions for an employee in the SAP payroll system. The system simply deducts payments in the sequence they are recorded in the employee master records. Procedures should be developed to ensure that high priority deductions (eg child support payments, garnishees, mortgage repayments) are deducted before less important deductions.

• The system should be configured to ensure that minimum payment amounts are specified for the various payment methods. A default payment method should be configured for payroll payments and the employee bank details should be specified as the required master file details for payment processing.

• 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.

• The ‘Run to run reconciliation report’ should be reconciled to the total of all payments processed for individual employees as well as prior period payroll totals, to ensure the accuracy of the payments processed. Any large or unusual payments should be further investigated.

**STANDARD FEATURES** SAP also has some standard features which help to ensure that gross and net pay are calculated correctly:

• The payroll area determines the employees to be included in the payroll run as well as the dates for the payroll accounting period.

• The exact payroll accounting period dates are determined by applying the payroll period definition (eg monthly, fortnightly) against the dates from the previous payroll accounting period which are stored in the payroll control record. If payroll processing is commenced without specifying a payroll accounting period, the system automatically determines the period by retrieving the previous period and incrementing this by one.

• An employee cannot be changed from one payroll area to another during a payroll period. This can only be performed at the end of a period.

• The system automatically calculates the total gross pay per employee on the basis of the wage types configured for inclusion in the total gross pay for an employee.

• It is possible for recurring payments and deductions to be assigned to different general ledger accounts/cost centres than the basic pay amounts. Additional payments can also be assigned to different accounts.

• The retroactive accounting date (the earliest date for which a retrospective payroll adjustment can be made) is determined by the system as the most recent of the date set per payroll accounting area, or the date set per employee in the payroll status record, or the date employment commenced for the employee.

• The system automatically performs ‘retroactive accounting’ if changes to master data or time data affect a previous payroll. The system checks whether the change is relevant for retroactive accounting to ensure that insignificant changes do not result in a retroactive accounting run.
• The system locks all personnel numbers for the relevant payroll area when the payroll area is ‘released’ for processing. This prevents any master data maintenance during payroll processing with the exception of master data changes that relate to a future payroll period.

• The transfer of payroll data to the FI/CO modules can only be performed if there were no rejections during a payroll run. All rejections must be corrected and reprocessed prior to transferring data to FI/CO.

• Tax scale is a required entry field and is used by the payroll program to determine the amount of tax to be paid on the employee’s gross salary. SAP contains the standard tax rates within tables and uses these to calculate the appropriate PAYE tax automatically based on the tax scale specified for the employee.

• The system automatically retrieves the payroll data that has been calculated by the system and uses this data to prepare the payment information. This is usually in the form of the CEMTEX tape which is prepared for download to the bank/payment authority.

• Once an employee has been terminated, their employment status is set to ‘0’. The system interprets this status and will not include the employee in subsequent payroll runs.
Liabilities are correctly calculated and accounted for

Provisions for annual leave and long service leave may not be correctly calculated, resulting in under- or over-payments of leave and inaccurate provisions in the financial accounts.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that liabilities are calculated correctly:

**Critical**

- The system incorrectly calculates long service leave liability by including a provision for employees who have been working with the organisation for less than the minimum qualifying period. In order to correct this over-provision it is necessary to run the 'Leave balances report' excluding employees with less than the minimum required amount of consecutive service and then raising an adjustment journal for the difference in the provisions. This adjustment should be performed by the finance department in the financial accounting module.

- 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 agencies.

- Leave accrual rules are used to calculate the leave accruals for each employee. The leave accrual rules should be consistent with employee awards.

**Important**

- 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'. Care should be taken during data entry as some versions of SAP will interpret the entry of '31.12.99' as the date '31/12/1999' which would result in the leave accrual rule expiring at the end of 1999.

- Maximum values (total value of the entitlement and accrual allowed) can be configured for each type of leave accrual. If the maximum leave accrual amount is reached, the system will stop accruing further leave and issue a message. A warning value can also be defined to warn the user when the predefined level is reached. However, leave will continue to accrue. These values should be configured appropriately to control each leave type in the system.

- The accounts posted for the superannuation liability should be appropriately configured to ensure that each employee’s superannuation contributions are processed on a timely basis.
SAP also has some standard features which help to ensure that liabilities are calculated correctly:

- Provisions for annual leave, long service leave and other employee benefits (e.g., sick leave) are automatically calculated by the system on the basis of leave accrual rules.
- Leave accrual balances are updated on a periodic basis depending on the leave accrual rules (e.g., each payroll period, annually).
- Superannuation contributions are automatically calculated by the system and posted to the relevant creditor account to recognise the employer contributions due on behalf of the employee.
Payroll payments are approved

Payments may be made without appropriate authorisation, resulting in overpayments or incorrect payments.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that payroll payments are approved:

- Authorisations provide the ability to restrict the access to process the payroll accounting run. This should be restricted to authorised payroll staff only.

**Important**

- The ‘Payroll exceptions report’ (refer to ‘Useful reports’ on page 135) should be reviewed after each payroll run to identify any new commencements or terminations. This may assist in identifying any new employees that have been included in the payroll accounting area without appropriate authorisation.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that payroll payments are approved:

- The payroll system automatically calculates a payroll payment for all employees who are included in the relevant payroll accounting area and who have an ‘active’ payroll status.
Payments are made to the correct employees

Payroll payments may be processed for the wrong employees or employees who do not exist on the organisation’s payroll records.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that payments are made to the correct employees:

- Changes made to the payroll status (infotype 0003) should be logged and reviewed to ensure that all changes are authorised. A change to the employee’s status could allow a terminated employee to be reinstated on the payroll and then payments could continue to be processed for the employee. Consideration should be given to developing a custom exception report to monitor this activity.

- Appropriate procedures should be implemented to ensure that the CEMTEX 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 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.

**STANDARD FEATURES**

SAP also has some standard features which help to ensure that payments are made to the correct employees:

- Employee bank account details are automatically retrieved by the system during creation of the payroll payments (CEMTEX) file.

- The payroll system automatically calculates a payroll payment for all valid employees.
USEFUL REPORTS

Payroll processing

- There are several reports which should be run as part of payroll processing. These reports can be found in the information system for HR (Human resources ➔ Payroll ➔ Info system ➔ Report selection):
  - ‘Payroll exceptions report’ - this report highlights any exceptions for the current payroll run as well as details of commencements and terminations. It should be produced as part of each payroll processing run to ensure that any payroll exceptions are identified and corrected before processing the payroll;
  - ‘Logged changes in infotypes’ - this report should be run at the commencement of each payroll processing run. Refer ‘Personnel/human resources functions’ section for further details;
  - ‘Employee pay details (payroll result) report’ - provides a complete list of all payments made to employees by the payroll run and should be reviewed to ensure payments are appropriate; and
  - ‘Payroll history (payroll payment) report’ - provides payroll history information and should also be reviewed for reasonableness.

Payroll payments

- Several reports are available to assist in performing the payroll payments function and can be found in the payroll information system (Human resources ➔ Payroll ➔ Info system ➔ Report selection):
  - ‘Run to run reconciliation report Australia’ - this report should be used to ensure that the year-to-date payroll figures are as expected. This report should be reconciled against the totals from the ‘Employee pay details report’ to ensure that all processing has been performed completely; and
  - ‘Bank deposit summary report’ - this report is produced when the payroll payment data files are created. It should be sent to the bank/payment authority for reconciliation against the data file received, to ensure that all payments are accurately updated to the employee bank accounts.

Leave Benefits processing

- There are several reports available via the standard HR information system (Human resources ➔ Payroll ➔ Info system ➔ Report selection) which should be reviewed by management on a regular basis to monitor leave balances effectively:
  - ‘Leave projection report’ - this report summarises leave accruals and payments for a point projected into the future. The report excludes terminated employees;
‘Long service leave projection report’ - this report summarises expected future long service leave provisions and payments for a point in time. The report excludes terminated employees as well as employees who have not been working with the organisation for a sufficient period of time to receive long service leave entitlements; and

‘Leave balances report’ - this report displays leave accrual and payment balances for the payroll period. It should be run before finalising the payroll to ensure that the leave balances for all employees are correct. The report excludes terminated employees.

Superannuation/taxation payments

- There are several reports available via the standard HR information system (Human resources ➔ Payroll. ➔ Info system ➔ Report selection) which should be reviewed by management on a regular basis to monitor superannuation information effectively:
  - ‘The Superannuation fund report’ - displays information relating to superannuation funds for specific payroll areas. It displays fund details as well as employer and employee contributions;
  - ‘The SGC month employee report’ - displays superannuation guarantee contribution (SGC) details for employees including details of employee earnings used to calculate the contribution, employer and employee contributions, and any highlight messages about the fund. The report only displays information if it is run at the end of the SGC month;
  - ‘The Superannuation employee report’ - displays superannuation information for the chosen employees for the payroll period, including member details and employer and employee contributions; and
  - ‘The ATO notification report’ - details the amount of the superannuation guarantee contributions shortfall for the year. The nominal interest amount is also shown as specified in the legislation. Administration amounts are also detailed on the report.

SECURITY CONSIDERATIONS

- Consideration should be given to implementing appropriate security measures over the transmission of payment data files to the payment authority/bank, and controls to ensure the accuracy and completeness of the transmission.

- Refer also to the ‘Personnel/human resources functions’ section.
Basis component and cross-application matters

SECTION CONTENTS

<table>
<thead>
<tr>
<th>Basis overview</th>
<th>139</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environment</td>
<td>140</td>
</tr>
<tr>
<td>Environment overview</td>
<td>140</td>
</tr>
<tr>
<td>Significant risks</td>
<td>141</td>
</tr>
<tr>
<td>SAP organisational structure</td>
<td>143</td>
</tr>
<tr>
<td>Design and system documentation</td>
<td>144</td>
</tr>
<tr>
<td>User training</td>
<td>145</td>
</tr>
<tr>
<td>Security implementation strategy</td>
<td>146</td>
</tr>
<tr>
<td>Data administration/ownership</td>
<td>147</td>
</tr>
<tr>
<td>Backup and recovery</td>
<td>148</td>
</tr>
<tr>
<td>Security</td>
<td>149</td>
</tr>
<tr>
<td>Significant risks</td>
<td>150</td>
</tr>
<tr>
<td>Configuration 'hot spots'</td>
<td>150</td>
</tr>
<tr>
<td>Security administration</td>
<td>151</td>
</tr>
<tr>
<td>System security parameters</td>
<td>153</td>
</tr>
<tr>
<td>Restricting access to data/programs</td>
<td>155</td>
</tr>
<tr>
<td>Restricting access to powerful system functions</td>
<td>156</td>
</tr>
<tr>
<td>System 'super users'</td>
<td>158</td>
</tr>
<tr>
<td>Restricting access to system tables</td>
<td>159</td>
</tr>
<tr>
<td>Segregation of duties</td>
<td>160</td>
</tr>
<tr>
<td>Useful reports</td>
<td>161</td>
</tr>
</tbody>
</table>
Change control ..........................................................................................................................................................................163
  Change control overview .....................................................................................................................................................163
  Significant risks ...............................................................................................................................................................164
  Configuration ‘hot spots’ ..................................................................................................................................................164
  Documentation, quality assurance and overall change control strategies ..................................................165
  Modifications to the SAP system ..............................................................................................................................167
  Useful reports ........................................................................................................................................................................168
  Security considerations ...............................................................................................................................................168

Interfaces with external systems ..........................................................................................................................169
  Overview ........................................................................................................................................................................169
  Significant risks ..........................................................................................................................................................170
  Interfaces from legacy systems ...............................................................................................................................171
  Interfaces to external systems (including download of data to diskette) .....................................................173
  SAP internal interfaces ..............................................................................................................................................174
  Useful reports ...............................................................................................................................................................175

Data conversion ..........................................................................................................................................................176
  Data conversion overview .......................................................................................................................................176
  Significant risks ..........................................................................................................................................................177
  Data conversion procedures ......................................................................................................................................178
Basis component and cross-application matters

Basis overview

The BASIS component is the core module of the SAP system and is used to perform system administration functions. It also encompasses system security and change control functions. Cross-application refers to administrative system functions that apply across all modules of the SAP system and are not unique to any one module.
Environment

The SAP environment refers to the technical aspects of the system implementation including system installation, security implementation strategy, data administration and ownership, and backup and recovery procedures.

Please note that some of the components of the above diagram are outside the scope of this handbook. As indicated in the introduction there are many risks associated with the SAP environment and many of these are specific to the particular combinations of technology platforms employed by the agency. Other ANAO better practice handbooks/guides will cover some of the components not within the scope of this handbook.
SIGNIFICANT RISKS

• A lack of systems/design documentation may result in difficulties maintaining the system, particularly if members of the implementation team subsequently leave the organisation.

• A lack of sufficiently detailed user documentation may result in users having considerable difficulty using the system. This may prevent the organisation from gaining maximum benefit from the system.

• Failure to invest in sufficient user training may result in users being unable to use the system properly. This may lead to an increased rate of errors and users may not fully accept the new system.

• The lack of a formal security implementation policy may result in a failure to implement adequate security controls.

• If data ownership is not clearly defined for the SAP system it could result in data integrity being compromised.

• A lack of backup and recovery procedures may result in system programs and data being lost in the event of a disaster. Inadequate disaster recovery and business continuity plans may also result in the agency being unable to function in the event of a disaster.

• There are numerous significant risks relating to the operating system and database management system used to support SAP (eg UNIX, Oracle). These risks should be separately considered based on the specific technology combination employed.

• Inadequate operating system and database management system security settings could affect the availability and integrity of application data as well as compromising the confidentiality of system data.

• Accountability for inappropriate actions may be removed if operating system access is provided via SAP.

• Global system security parameters could be compromised if direct update of the SAP system profile parameters is performed via operating system utilities.

• Access to the standard users at the SAP, operating system and database management system levels should be restricted to ensure that the integrity of system data and programs is protected. Standard users include:
  - SAP:
    - SAP*
    - DDIC
    - SAPCPIC; and
    - Earlywatch.
  - Operating system eg (UNIX):
    - root
    - <SID>adm; and
    - <DB><SID>.
  - Database management system:
    - SAPR3.

continued...
• Unauthorised access may be gained to the system when using the R/3 online services via the SAProuter. User profiles should also be set up that are tailored to the type of access required.

• Access to create new clients should be adequately restricted to prevent users from creating new clients and logging on as SAP*. This could also potentially allow access to client-independent data held in existing clients.
SAP organisational structure

Failure to adequately define the SAP organisational structures to be used for the organisation could prevent the system from providing useful information.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that the organisational structure implemented meets the organisation’s needs:

- SAP provides a flexible organisational structure which can be adapted to virtually any organisation. The organisational structure implemented in SAP should be designed to represent the organisation accurately. The organisation should assess which SAP structures would best meet their needs with due consideration to the need to secure access to various organisational structures. For example, different legal entities should be represented as separate ‘company codes’ within SAP as this allows separate statutory reporting and access to individual company codes can then be restricted. Consideration should also be given to which organisational units might be used for segregating reporting and responsibilities within the organisation (eg business area, cost centre, plant, sales organisation).

- Consideration should also be given to the frequency of change for organisational structures within the system. Significant changes to certain organisational structures may be difficult or inefficient to implement. It should also be noted that the system is unable to support security restrictions for some organisational entities (eg storage location).
Design and system documentation

Inadequate design and system documentation may result in the system being difficult to maintain.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that the system is able to be maintained and used with ease:

- Adequate user and systems documentation should be developed prior to implementation. The documentation should include the SAP-supplied documentation as well as organisation-specific documentation covering (but not limited to) the following areas:
  - design documentation of the key business processes including automated and manual control procedures and the configuration settings implemented, including all options considered along with the reasons for choosing the selected settings;
  - user documentation for key business processes outlining the screens and transactions involved and the required data input;
  - design documentation describing the development of SAP access profiles; and
  - documentation describing development of custom programs and reports.

- Procedures should be implemented to ensure that user and systems documentation is maintained and kept up to date. This should include revisions for any upgrades to the SAP software as well as changes as a result of any new functionality implemented or changes to business processes. These procedures should also be incorporated as part of the change control procedures.

- Any modifications to the standard SAP system should also be adequately documented and tested. Modifications to the standard system should only be made if the system cannot meet a key business requirement and other work-around solutions are not suitable.

- Custom developed ABAP programs should be well documented and should be thoroughly tested in the development environment prior to implementation.

- The documentation features in the Implementation Guide should also be used to ensure that configuration settings implemented are adequately documented to assist in future maintenance of the system.
User training

Failure to provide comprehensive training for users could result in users having considerable difficulty in using the new system. It could also result in users rejecting the system and/or failing to obtain maximum benefit from the system.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that users are able to use the system competently:

**Critical**

- Management should ensure that an appropriate investment is made in training courses for all staff who will be using the new SAP system. The implementation of SAP represents a significant organisational change and it is essential that this process of change is successfully managed to minimise the impact on employees. Training should cover all aspects of the system for which users will need to be skilled and should be supported by thorough user documentation which includes information on system usage, business procedures, and a reporting manual.

**Important**

- A post-implementation review should be performed to assess whether the system has been implemented as intended and is meeting all of the requirements of the organisation. A post-implementation review assists in identifying any potential configuration or business process problems with the system implementation.
**Security implementation strategy**

The lack of a formal security implementation policy may result in a failure to implement adequate security controls. This occurs in many implementation projects where security is merely an afterthought, and results in the implementation of an insecure system.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that appropriate controls are incorporated in the system implementation:

- A formal security implementation strategy should be developed and should be followed during implementation to ensure that appropriate security controls are implemented. The strategy should include at least the following elements:
  - a task list documenting all processes involved in the design, development and implementation of security, including details of specific responsibilities for each task;
  - a detailed implementation timeline outlining the estimated start and completion dates;
  - supporting documentation outlining in detail each of the processes identified in the task list;
  - checklists to ensure that no required design, development or implementation processes are overlooked;
  - naming conventions that have been adopted; and
  - details of any tools and accelerators (eg Profile generator) that have been used.

- The security implementation strategy should also take into consideration the need to effectively segregate conflicting functions and roles within the system.

**Important**

- Appropriate security procedures should be implemented to ensure that information technology staff are prevented from gaining access to SAP transaction data and programs in the production environment.

- A detailed security policy should be implemented to control access to the SAP infrastructure including the operating system, database management system and the local area network.

- Access to perform system development and configuration tasks should be removed from all users in the production environment prior to the implementation ‘go live’ date.
Data administration/ownership

If data ownership is not clearly defined for the SAP system it could result in data integrity being compromised. It increases the risk of unauthorised users receiving access to sensitive system data. A lack of responsibility for data ownership could also cause delays in addressing system errors or correcting erroneous data.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that data ownership is clearly defined:

**Critical**

- SAP program and data ownership should be formally identified and assigned to a specific role in the organisation.
- 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.

**Important**

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

Lack of an adequate backup and recovery strategy could result in the system and the data contained in it being lost in the event of a disaster.

**BEST PRACTICE PROCEDURE**

*Best practice procedures which could be implemented to ensure that adequate backup and recovery procedures are performed:*

**Critical**

- Clearly documented procedures should be in place to mandate the regular backup of the system. System backups should be performed on a daily basis and backup media should be stored off-site for maximum effectiveness.

**Important**

- Backup and recovery procedures should be tested regularly to ensure compliance with the procedures and to make any improvements considered necessary.
- A comprehensive disaster recovery plan and business continuity plan should be developed to ensure that the organisation can continue to operate in the event of a disaster. These plans should include, but not be limited to covering, the IT systems.
Security

Many aspects of SAP security need to be considered. These include security administration, maintaining global security parameters, securing access to data and programs, restricting access to standard profiles and authorizations, limiting the use of super users, protecting access to system tables, and segregating functions within the system. SAP provides an 'Authorizations Infosystem' to assist in managing security administration.
**SIGNIFICANT RISKS**

- Access to security administration functions may not be adequately restricted in all environments.
- Activity groups/profiles and authorizations may be maintained directly in the production environment. This increases the risk of error and unauthorised changes as the profiles and authorizations will not be subject to an appropriate review.
- Security administration staff have the ability to maintain their own access privileges and may therefore be able to access all transactions.
- Unauthorised users are able to gain access to the system using the default passwords of standard system user master records.
- Custom transactions and programs are developed without including the appropriate security checks.
- Users are able to access the operating system command line from within SAP.
- Users have been allocated powerful standard SAP profiles and authorizations.
- Users are able to execute any ABAP program in the system.
- Developer access rights are provided in the production environment.
- Access is provided in the production environment to table-maintenance functions including client independent table maintenance.
- Profiles and authorizations have been granted to users without any consideration of the implications of conflicting duties.

**CONFIGURATION ‘HOT SPOTS’**

- Ensure suitable settings for system profile parameters for:
  - log-in failures before user lock;
  - minimum password length; and
  - password expiration.
- Activate the SAP* safety net (login/no_automatic_user_sap*).
- Ensure disabling of authorization checks has not been used inappropriately.
- Change passwords of SAP-delivered user master records from defaults in all clients.
Security administration

Failure to implement adequate SAP security administration procedures could result in unauthorised access to sensitive data and programs, affecting the integrity, availability, or confidentiality of the system and its data.

Best practice procedures which could be implemented to ensure that access to the system is restricted to authorised users:

- Access to perform security administration functions including the profile generator should be restricted. This is controlled via the following authorization objects:
  - User master maintenance: User groups;
  - User master maintenance: Authorization profile;
  - User master maintenance: Authorizations;
  - Authorization check for transaction start.

- SAP security may be administered in a centralised or decentralised manner (ie at one location or many). In both cases 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);
  - authorization administrator (maintains profiles/activity groups and authorizations); and
  - activation administrator (activates/generates profiles and authorizations).

  Authorization and activation administration should be performed in the development environment. Segregation of the activation and authorization 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 authorizations.

- Security administrators may grant themselves access to inappropriate transactions. They can be restricted from maintaining their own access rights but would still be able to create a new user master record which they could use to access the inappropriate transaction. Security administrator access can only be fully restricted if SAP is linked to an external security system (eg SECUIDE or KERBEROS).

  Review of all security maintenance and/or transactions accessed by the security administrator can provide an adequate level of control.
Desirable

• A periodic review should be performed of the access rights assigned to each user, to ensure that an adequate segregation of duties is maintained.
System security parameters
Password and log-on controls assist in protecting the system from unauthorised access attempts. Inadequate settings could result in system security being compromised and also increases the risk of unauthorised access being gained to the system.

**BEST PRACTICE PROCEDURE**
There are a number of system security parameters which can be set to enhance security:

**Critical**

- User master records should be locked after a certain number of unsuccessful attempts to log-in to the system with an incorrect password (e.g., three attempts). This protects against an unauthorised user continually attempting to guess another user’s password. Locked user-ids are automatically unlocked at midnight and a daily review of locked users is therefore recommended. This can be achieved via review of the system log or a scheduled report of the locked users (run immediately prior to the automatic unlocking).

- If the SAP* user master record is deleted, SAP* reverts to its original state with complete access and a default password. A system parameter can be set to prevent users from being able to log on as SAP* with the default password in the event that the SAP* user master record has been deleted.

- Users should be forced to change their passwords at regular intervals (e.g., every 30 days). This reduces the likelihood of a third party gaining unauthorised access to the system.

- The minimum password length should be set to an appropriate value (e.g., six characters) to prevent passwords being guessed. The default system setting is three characters and the maximum length is eight characters.

**Important**

- SAP should stop the current session after a certain number of unsuccessful attempts to log-in to the system (e.g., three attempts). This may deter an unauthorised user from attempting to guess another user’s password.

- Users should be logged off the system after a specified period of inactivity. This may prevent an unauthorised user from gaining access to an idle terminal if the workstation has been left unattended for an extended period of time. It should be noted that the SAP auto log-out facility does not operate particularly effectively and experience has shown that a time-out period shorter than about 20 minutes is generally not practical. Time-out facilities at the local area network level should therefore also be utilised.

- It is possible to disable the system checking a user’s authorization for a transaction code at the commencement of each transaction. This check is turned on by default and should not be deactivated.
• If the profile generator is activated, it is possible to disable standard authorization checks. If used inappropriately this could create significant access exposures. This functionality should therefore be appropriately secured and changes closely scrutinised.

**Desirable**

• *Prohibited passwords can be defined in the system so that easily guessed passwords are prevented from being used.*
Restricting access to data/programs

Inappropriate access to SAP data and programs could result in unauthorised changes being made to system data including the processing of fraudulent transactions.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that access to SAP data and programs is adequately restricted:

### Critical

- Any custom transactions or programs that are developed should follow a consistent naming standard which complies with SAP conventions. It should be ensured that custom transactions and programs have the necessary access control checks included within them.

- SAP supplied user master records are very powerful and are delivered with default passwords. These passwords are well known and should be changed immediately to ensure the system is protected from unauthorised access attempts. Refer to ‘Useful reports’ on page 161. These user-ids are the first to be attempted by unauthorised users, such as hackers, trying to break into an SAP system.

- There is a standard SAP program which allows the user to access the operating system command line. This enables the user to perform operating system commands from within SAP using the powerful access rights of the SAP user-id in the operating system. There is also a standard transaction which allows access to perform a pre-defined set of operating system commands as well as creating and executing new commands. Access to these utilities should be restricted from all users in the production environment. Operating system access should be administered via the operating system itself and not from within SAP.

### Important

- 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.

- 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.

### Desirable

- *Any sensitive transactions that are not used can be locked in the system to prevent intentional or unintentional use.*
Critical

- SAP comes with a number of standard profiles and authorizations which can be used by the organisation. These standard profiles and authorizations should not be used in production because they provide very generic access and generally do not adequately address segregation of duties issues. These standard profiles and authorizations are also subject to changes in future releases of SAP which may result in changes to user access rights after the software is upgraded.

- Users should be restricted from executing ABAP programs in the production environment. There are many powerful ABAP programs in the system which perform sensitive functions (e.g., deleting master data) yet do not incorporate any security checks. Access to the transactions used to nominate then execute ABAP programs (including ‘Report painter’) should be restricted. 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 authorization group and access restricted via authorization group using the authorization object ‘ABAP/4: Program run checks’.

- Access to development functions including the ability to maintain ABAP programs should be totally restricted in the production environment. This is controlled via the authorization object ‘ABAP/4 Development workbench’ which (apart from display access) should not be allocated in production.

- There are various powerful standard profiles in the system which should not be granted to users including:
  - ‘All authorizations for the R/3 system’ (SAP_ALL): 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.
  - ‘All authorizations for newly created objects’ (SAP_NEW): this profile provides general access to any new profiles and authorizations which are included in a new release of SAP. These may provide access to inappropriate functions. Some documentation suggests granting this access to all users, however, this would be inappropriate and could seriously compromise security. Procedures should exist to review and test new objects which become available before allocating them to users. This profile should not be allocated to any users in production.
**Important**

- Debug access should not be provided to any users in the production environment. This could allow a user to bypass the authority checks included in ABAP programs/transactions.

- Access to perform corrections and transports should be restricted in all environments. This access is provided by the authorization object 'Workbench organizer and transport system' which should be granted to authorised users only. Refer to 'Security considerations' on page 168.

- Access to the 'System Administration Functions' authorization object should be restricted as this provides users with access to powerful systems administration functions including the following:
  - creating new clients;
  - locking / unlocking transactions;
  - controlling spool (print) requests; and
  - deleting data without archiving.

- Access to the batch processing authorization objects should be restricted, as these provide access to background job administration functions. These functions should be restricted to authorised users only.

- Access to maintain ABAP program attributes and copy or delete programs should also be restricted from unauthorised users via the authorization object 'ABAP/4: Program run checks'.

**Desirable**

- The ability to run and maintain queries in the production system should be restricted to authorised users via the authorization object 'Authorization for ABAP/4 query' in order to protect confidential data.
**System ‘super users’**

Super users have powerful system access rights and should be adequately protected to ensure that unauthorised access to the system is prevented. If access is gained to super user accounts it could result in unauthorised transactions being processed and the integrity of system data being compromised.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that super users are adequately controlled in the SAP system:

- 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 recommend 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.

- Default passwords for the standard SAP-delivered user master records should all be changed to prevent unauthorised access to the system.

- The combination of powerful profiles which are assigned to SAP* should not be assigned to any other single user master record with the exception of the user created to replace the SAP* user master record.

- Policies and procedures should be developed to ensure access to ‘super users’ is adequately restricted. Procedures should include the storage of super user account passwords in a secured location (e.g. safe) and processes to require the changing of the password after each use. The activity of super user accounts should also be monitored to ensure that access is used only for appropriate purposes.

- The SAP system is delivered with a standard user master record called ‘EARLYWATCH’ which is used by SAP to provide an optional online support service. This user is assigned all authorizations for the SAP system which is an inappropriate level of access to the organisation’s programs and sensitive data. This user and any other user master record accessed by SAP should be restricted to required functions only.
Restricting access to system tables

Changes to system tables in SAP are similar to performing a program change in legacy computer systems. Unauthorised access to the table maintenance function could result in system data and configuration settings being corrupted.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that unauthorised table changes are prevented:

**Critical**

- Specific transactions exist which allow direct updating of tables. Access to such transactions must be restricted only to authorised users through the authorization object ‘Table maintenance’.

- Some tables are client-independent which means that if they are updated in one client this affects all SAP clients in the same environment (system). Access to maintain client-independent tables for non-production clients which reside on the production client machine should be restricted. Access to maintain client-independent tables is provided by the authorization object ‘Maintenance of client-independent tables’.

**Important**

- 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 care should be taken when assigning access to maintain tables in the class ‘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 (e.g., HR tables). This access should be restricted by table class.

- Access to data dictionary (system tables) transactions 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.

- 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.
Segregation of duties

Certain combinations of profiles or authorization objects within a user master record may allow a user to process transactions which, in combination, result in a compromise of segregation of duties.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that conflicting responsibilities are segregated in the SAP system:

- As part of the security implementation project, the profiles being designed should be assessed to determine whether they provide access to conflicting duties in the system. Care should be taken to ensure that the activity groups/profiles created provide only the level of access which is intended by management. A job roles matrix should be developed as part of the security implementation strategy to ensure that the roles assigned to each ‘job’ or ‘position’ in the SAP system are clearly defined.

- Procedures should be developed for user administration to ensure that segregation of duties issues are considered. These procedures should ensure that:
  - new users are not granted any combination of profiles/activity groups that would result in them having access to perform functions which are not consistent with their job role or position in the organisation (eg a purchasing officer having the ability to post an invoice); and
  - the access rights of existing users are assessed prior to new profiles/activity groups being included in their user master records. The allocation of a new profile/activity group may result in the user having inappropriate access to functions which are inconsistent with their job role. It may be necessary to remove existing profiles/activity groups from the user master record.

**Important**

- A periodic review should be performed to evaluate the levels of access that have been granted to system users. This may be performed manually or with the aid of third party software tools. The aim of the review should be to identify any potential conflicts in the users’ access rights and to ensure that these are corrected.
USEFUL REPORTS

There are a number of reports which should be used to assist in managing the security function within SAP. These reports can be accessed via the authorizations infosystem report tree (Tools ➔ Administration ➔ Maintain users ➔ Repository Infosys). Some of the reports listed should be reviewed on a regular basis while others may be useful for ad hoc queries:

- **'Current active users'** - lists users that are currently logged onto the system and the transaction they are currently executing;
- **'Users according to complex selection criteria'** - allows searching for users according to complex criteria including profiles, authorizations, and authorization objects. This may be useful in reviewing the level of access granted to a particular user. Similar reports are available for profiles and authorizations;
- **'Check passwords of SAP* and DDIC in all clients'** - performs a check of the passwords of standard SAP user-ids to ensure that the default passwords have been changed;
- **'Users with critical authorizations'** - prepares a list of all users with pre-defined critical Basis authorizations including batch administration, spool management, security administration, table maintenance, and the transport system;
- **'Users locked due to incorrect log-on'** - lists all users that have been locked due to exceeding the number of permitted log-on attempts;
- **'Transaction access lists'** - provides a list of the transactions that can be executed by a particular user or with a selected profile/activity group;
- **'Comparison tool'** - compares two different security components (users, profiles, or authorizations) in the system;
- **'Where used lists'** - provide a useful report detailing in which user master record, profile or authorization a particular profile/authorization/authorization object is used; and
- **'Change documents'** - these reports provide a change history for the selected users, profiles, or authorizations and provide a number of selection criteria. These reports are more useful than the standard change document reports available in the system because they allow a query to be run to detect all changes over a given period of time. The standard change documents (Tools ➔ Administration ➔ Maintain users ➔ Users ➔ Information ➔ Change documents ➔ ...) only allow changes to be reported for specifically identified security components.

It should be noted that the reports listed above do not always provide an entirely accurate picture of system security as many of the reports perform queries based only on the 'Authorization for transaction start' authorization object. This ignores the fact that a user requires further objects in order to execute a transaction.
Several other reports are also available which may provide useful information in the management of the security administration function:

- **‘SAP system log’** - this report is executed via the menu path Tools ➔ Administration ➔ Monitoring ➔ Performance ➔ Exceptions/users ➔ Exceptions ➔ System log. It is a useful system administration report and includes details of locked user master records; and

- **‘Statistics records’** - this report is executed via the menu path Tools ➔ Administration ➔ Monitoring ➔ Performance ➔ Workload ➔ Statistics records. This report provides information about the transactions/programs that have been accessed by the selected user and could be of assistance in monitoring the activity of ‘super users’.
Essential to ensuring the integrity of any system is a well defined change control process. SAP incorporates its own change control system – the correction and transport system (CTS). The CTS is used for transporting changes to SAP objects (eg programs, tables) between the various SAP clients and environments in a controlled manner. The CTS helps to ensure that only authorised changes are applied to the production system.
SIGNIFICANT RISKS

- Development or test clients may reside on the production system, compromising the integrity of client-independent programs and data.
- Change control procedures may not exist, resulting in changes being applied directly to the production environment and without adequate testing.
- Objects may be moved between SAP clients using operating system utilities without using the control mechanism provided by the CTS.
- Developers may have access to use the CTS and therefore bypass quality control procedures.
- Developers may have access to modify CTS configuration tables and override CTS control settings.
- Changes may be permitted to tables, programs and other objects in the production and test clients.

CONFIGURATION ‘HOT SPOTS’

- Ensure that the system change options are set to ‘Objects cannot be changed’.
- Ensure that the client change settings are set to prevent changes to client-dependent and independent objects and that critical clients (eg production) are prevented from being overwritten by copying.
- Critical customising and CTS tables should be logged. Ensure that table logging is activated at a global level and for each individual table to be logged.
- Ensure that key CTS tables are appropriately configured and consistent across each environment to ensure the successful operation of the CTS.
Documentation, quality assurance and overall change control strategies

A lack of clearly defined change control procedures could result in unauthorised changes being applied to the production SAP system without adequate testing.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that changes are made to the system in a controlled and systematic manner:

1. The SAP architecture that is implemented should provide separate environments for development, testing and production (refer to the previous diagram) in order to support a separation of activities between developers and end users. An 'environment' may be a separate physical system or it may be a separate 'instance' on the one physical machine. A migration path should be defined between the three environments that supports the use of the CTS. All development tasks including creation/maintenance of programs, system settings, and master data should be performed in the development environment.

   These should then be 'transported' to the test environment using CTS where they should be subject to thorough unit and integration testing to fully assess the impact of the changes. Any further development work identified as a result of testing should be performed in the development environment and then transported back to the test environment to be tested again. If the test results are positive and the change is ready to be loaded into production, the objects should be transported to the production environment using CTS. No utilities other than the CTS should be used to move objects and data between SAP systems. The test and production clients should never reside in the same instance.

2. Comprehensive change control procedures should be documented to ensure that all changes are performed according to consistent standards. Procedures should address all aspects of change control for the SAP system including the following:
   - 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;
   - other change management documentation;
   - review and approval procedures;
   - use of audit trail reports; and
   - testing requirements.
**Important**

- Quality assurance (QA) procedures should be defined for the change control process to determine the overall impact of changes to configuration, master data, and programs. The QA role should be separated from the role of developing the changes to ensure an independent review. Unit testing should be performed in the development environment and integration/user acceptance testing should be performed in the test environment. End users should be involved in testing and should be required to signoff on any changes to the system. Testing procedures should also specify the source of data to be used for testing to ensure that test results are realistic.

- Changes to configuration objects should be documented. These are usually transported via CTS but can also be updated online in production. If changes are made online, approval and review procedures should be in place and changes should be tested in the test environment before being applied directly in production.

- Some configuration objects cannot be transported (e.g., number ranges, company codes). All changes to such objects should be documented and reviewed.

- Pre-approval procedures should be in place before any changes to development objects and configuration elements are made either online or transported. There should be an adequate segregation of duties to ensure that only approved changes are migrated to production.

- Changes to sensitive system customising tables (including CTS tables) should be logged in the development environment and the report 'Analysis of table log database' reviewed on a regular basis to assist in providing a quality assurance review of any changes performed.
Modifications to the SAP system

If changes to objects and configuration are not adequately protected the integrity of system programs and data may be seriously compromised.

**BEST PRACTICE**

**PROCEDURE**

Best practice procedures which could be implemented to ensure that changes made to system objects and configuration are authorised:

**Critical**

- Access to the workbench organizer 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 organizer. These tables should be restricted in all environments. Refer to ‘Restricting access to system tables’ on page 159.
- 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.
- All production and test clients should be set to prevent changes to client-independent tables to ensure the integrity of system data.
- 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.
- All production clients should be protected against being overwritten by a ‘client copy’ operation.
- 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 which should include regular review of the table change report. Refer to ‘Restricting access to system tables’ on page 159. Developers should not have access to the CTS tables in any environment as this would allow them to override the CTS configuration settings.

**Important**

- Emergency repairs in the production system should be restricted and should only be performed if absolutely necessary.
- Settings in the CTS configuration tables should be consistent across all environments to ensure the correct operation of the CTS and the organisation’s change control procedures.
- 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.
USEFUL REPORTS

There are many standard reports available in SAP that can be used to assist in monitoring the change control process. Some useful reports which could be used include:

- ‘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’ reviewed on a regular basis to ensure that any unauthorised table changes are detected.

SECURITY CONSIDERATIONS

Access to the correction and transport system (CTS) should be restricted to authorised users only. This is controlled via the standard authorization object ‘Workbench organizer and transport system’ which provides access to the workbench organizer transactions including the ability to release objects for transport. Developers should not have access to the CTS or CTS configuration tables in any environment.

Developers should also be restricted from access to the ‘system change options’ settings, as changes to these settings may allow them to perform changes in the system.
A typical SAP system may have many interfaces from existing legacy systems as well as interfaces to other external systems. Inbound interfaces to SAP from legacy systems usually consist of a file which is sent from the legacy system to SAP and processed in the background via a standard SAP transaction. Outbound interfaces from SAP to external systems usually consist of a file which is sent from SAP to the external system and processed at periodic intervals by the external system. Alternatively, users can download data from SAP to their PC and then process it as they wish, for example, in a spreadsheet.

Appropriate procedures need to be implemented to ensure the use of interfaces is well controlled and to protect the integrity of system data.
SIGNIFICANT RISKS

- Data interfaced from legacy systems into SAP or from SAP to external systems may not be completely transferred or the files loaded may be corrupted.
- Unauthorised changes may be made during batch input error correction.
- Unauthorised changes may be made to batch input (interfaced files) without detection.
Interfaces from legacy systems
Failure to monitor or control interfaces from legacy systems may result in the file not being received completely or the file containing incomplete or corrupt data.

**BEST PRACTICE PROCEDURE**
Best practice procedures which could be implemented to ensure that interfaces are processed completely and accurately:

- Procedures should be in place to ensure that errors which may have occurred during the processing of the background session are corrected on a timely basis. Only authorised users should have access to correct batch input sessions. Users should be restricted by session name or some other means to prevent them from processing corrections to sessions which they are not responsible for. The system log can be reviewed to determine whether errors have occurred.

- Procedures should be implemented to identify any changes made to data during the correction of a batch input session. Such changes should be traced back to the legacy system or some other form of correction authorisation to ensure they are appropriate. Although SAP does not automatically log this type of information, there are various third party tools available which can assist in this process.

- Data interfaced to SAP from legacy systems should be reconciled to the source system to ensure the accuracy and completeness of the database. Reports used for this purpose should include control totals as well as record/transaction counts.

**Important**

- All interfaces into SAP from legacy systems should be identified. Information which should be gathered includes:
  - name / platform of the external system;
  - SAP transaction being processed;
  - frequency of processing (ie hourly, daily, weekly, monthly); and
  - any particular controls which relate to the interface.

- A specific SAP ‘document type’ should be defined for documents posted in the background from a legacy system to distinguish from documents which have been posted online in SAP.

- The job log should be reviewed after each batch run and errors corrected. Each job has an associated job log.

- Procedures should be implemented to ensure that duplicate batch files are not processed and that a file is not missed. This may include use of time schedules, date/time stamp tracking, and batch sequence numbers.

- Sequence checking should be performed to ensure that missing interface files are identified and followed up.
The process which transfers the interface file from the legacy system to the SAP system may contain a hard-coded username and password at the operating system level to enable the file to be transferred. This should not be allowed, as an experienced user may be able to obtain the username and password and subsequently create, modify or delete interface files.

Adequate security should be implemented to protect files when they are in an intermediate stage between the legacy system and the SAP system.

Desirable

A positive acknowledgment scheme may be used to ensure that files sent from a source system are received by SAP (ie a 'handshake' between the systems so that files are not skipped or lost).
Interfaces to external systems (including download of data to diskette)

The file(s) interfaced to the external system may not be completely processed by the receiving system or may contain incomplete or corrupt data.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that interfaces from SAP are processed accurately and completely:

- **Critical**
  - Procedures should be in place to identify any instances where the file interfaced from SAP has not been sent completely or received by the external system.
  - Information downloaded from SAP to external systems should be accompanied by control/reconciliation reports to enable the data sent from SAP to be reconciled against the data loaded by the external system (e.g., payroll payment data sent to the bank). The control reports should include details of the number of records/transactions interfaced (record count) and the control total (total cumulative amount) to enable easy reconciliation.

- **Important**
  - All interfaces to external systems from SAP should be identified. Information which should be gathered includes:
    - name / platform of the external system;
    - SAP data being sent;
    - frequency of processing (e.g., hourly, daily, weekly, monthly); and
    - any particular controls which relate to the interface.
  - A policy should be established to outline the controls that should surround the process of downloading data from SAP to a diskette. As this process is controlled by the individual user, there are unlikely to be any automated system procedures in place to ensure that all data is downloaded correctly. Procedures should outline user responsibilities including restrictions on the use of sensitive information and the need to perform a reconciliation of the data downloaded to the data contained in SAP (e.g., reconcile on control totals and record counts).
  - An automated process may be used to transfer the interface file from the SAP system to the external system. In this case, a hard-coded username and password to log into the external system may exist in the procedure which enables the file to be transferred. This should not be allowed, as an experienced user may be able to obtain the username and password and subsequently create, modify or delete interface files.
SAP internal interfaces

SAP internal interfaces may not balance due to incorrect coding and allocation of accounts.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that internal interfaces are balanced:

- The ‘Financial accounting comparative analysis’ report should be reviewed as part of month-end procedures to ensure that general ledger accounts are in balance with the various sub-ledgers.

- Procedures should be in place to ensure that appropriate reconciliation accounts are entered as sub-ledger control accounts in master records. This will ensure that sub-ledgers remain in balance with the general ledger.

**STANDARD FEATURES**

SAP standard functionality to ensure that internal interfaces are balanced:

- All modules within SAP are fully integrated and automatically interfaced. As a result traditional batch total controls are not required.

- SAP uses reconciliation accounts to control the balancing between sub-ledgers (eg accounts payable) and the general ledger. Direct postings cannot be made to reconciliation accounts.
USEFUL REPORTS

- The ‘Financial accounting comparative analysis’ report should be regularly reviewed to ensure that the reconciliation accounts in the general ledger balance with the sub-ledgers.

- The report ‘Batch input: display logs’ should be reviewed after each batch input session to determine whether any errors occurred during the processing of the batch input session.
An integral part of any SAP implementation project is the conversion of data from existing legacy systems into a format that will be recognisable by SAP. Data conversion involves the loading of all starting balances and master data into SAP. This may also involve data cleansing prior to the conversion process.
SIGNIFICANT RISKS

- There may not be a data conversion strategy to deal with the conversion of individual data entities such as open purchase orders or partly delivered purchase orders. This may lead to a breakdown in control procedures for these transactions.
- The data that is loaded into SAP may not be good quality and may result in corrupted transaction and master file databases in the new system before it is ‘live’.
- Inadequate reconciliation procedures may be in place to ensure that all data from the legacy system is actually converted into SAP data.
- Testing procedures may not be sufficient to ensure that all data conversion routines are operating as expected.
- There may be no procedures in place for the collation of data required by SAP that is not currently stored in the legacy systems.
- Purchase order conversion is a common source of problems, due to the variety of purchase order scenarios that may exist at the time of conversion.
**Data conversion procedures**

During the data conversion process records may be lost or corrupted resulting in erroneous data being loaded into SAP. Inadequate data conversion procedures may also result in data being omitted from the data-load process altogether.

**BEST PRACTICE PROCEDURE**

Best practice procedures which could be implemented to ensure that data conversion is completely and accurately performed and that all data loaded into SAP is valid:

- Comprehensive conversion planning should be carried out and include the following:
  - identification of each data entity that needs to be converted;
  - identification of the staff responsible for each conversion project;
  - documentation of the conversion timetable including testing dates and time frames for the actual conversion processing; and
  - all conversion dependencies (i.e., conversions of data which are dependent on prior data entities having been converted) should be identified and documented prior to commencement of the conversion project to ensure that all conversions can be completed successfully.

- A data cleansing exercise should be completed prior to data conversion to ensure that all data to be converted is valid and current. Detailed documentation of any data cleansing which has occurred should be retained including lists of records which were not converted and records which were modified.

- Procedures for the reconciliation and validation of all converted data should be documented. Procedures should include reconciliation of totals as well as detailed random testing of individual records. This should assist data conversion staff in ensuring that all data entities are completely and accurately converted.

- Data conversions may be performed via an automated routine (i.e., using SAP batch input programs) or manually. If an automated conversion approach is taken, the following additional procedures should be implemented:
  - Control reports should be produced from both the source system, SAP and any interim system used for conversion so that record counts and control totals can be compared to ensure the accuracy and completeness of the data conversion;
  - Records which were not converted due to errors in the batch session should be automatically reported including totals to assist with reconciliation;
  - Procedures should be documented outlining how to correct these errors and any changes made to data should be documented to provide an audit trail;
  - It may be necessary to set up SAP tables to be referenced during the automated conversion. The conversion procedures should document the process for maintaining these tables; and
All conversion and upload programs, as well as reconciliation procedures, should be comprehensively tested and testing should be signed off by user representatives. Test results should be documented to assist in following up any problems identified.

If a manual conversion approach is taken then the following procedures should be implemented:

- Input forms or some alternative source of data input need to be prepared to ensure the data is in a format recognisable to SAP;
- Any rejected input should be documented and corrected on a timely basis. Any changes made to the data should also be documented to provide an audit trail;
- An independent review should be undertaken to ensure that the data input is accurate and free of keying errors; and
- There should be procedures in place for the collation of data required by SAP that is not stored in the legacy system. Any new information that is loaded into SAP should be approved by an authorised employee and verified against the source documentation.
- Comprehensive testing of all data conversion procedures (including reconciliations) should be performed prior to the actual data conversion being performed.
- Access to transactions or movement types which are relevant only for initial data loading should be revoked following successful conversion reconciliation.

**Important**

- Data entities that are likely to cause conversion difficulties should be identified early in the conversion project and procedures designed to address these issues. For example, outstanding/open purchase orders may not be converted and paid out of the legacy system, they may be converted and paid out of SAP, or they may not be converted but paid out of SAP (a potential issue is that the invoice cannot be matched against the purchase order in this scenario). Conversion of partly delivered purchase orders is another significant issue for some data conversion teams.
- Documented procedures should exist to describe the process to be followed in maintaining both legacy system and SAP master files (parallel maintenance) if there will be a parallel running period for the two systems.
- Ownership of the converted SAP data files should be assigned so that user sign-off and acceptance procedures can be established.

**Desirable**

- Involvement of personnel external to the organisation (eg temporary staff) should be kept to a minimum and data input by temporary staff should be subject to additional checking.
Appendix 1

SECTION CONTENTS

Organisational structures in SAP ................................................................. 182
The implementation guide ........................................................................... 184
Numbering in SAP ..................................................................................... 185
Sub-ledger reconciliations ........................................................................ 185
Document types and postings keys ............................................................. 185
Validations and substitutions .................................................................... 185
Field status ................................................................................................ 186
Document changes rules ........................................................................... 187
Reporting and report trees ....................................................................... 187
Audit trails and logging ............................................................................. 189
Introduction to SAP security concepts ...................................................... 190
Appendix I: Introduction to SAP concepts

Reference has been made throughout the handbook to various SAP R/3 concepts. In order to assist the reader in understanding these concepts the following section contains a brief introduction to some of the concepts fundamental to the SAP system.

Organisational structures in SAP

Organisational structures must be defined in SAP to represent the structure of the organisation. These structures can be defined independently for each functional area of the system. For example, the sales department will want to define sales organisations, distribution channels and divisions (product groups), while the purchasing department will want to define purchasing organisations, plants and storage locations. Independent of these structures, a structure must be defined in financial accounting (FI) that represents the legal reporting entity. This structure is represented by the company code. The balance sheet and the profit and loss statement are prepared for the company code.

Functional areas and organisational structures include:

<table>
<thead>
<tr>
<th>Functional area</th>
<th>Organisational structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales and distribution</td>
<td>Sales organisation, distribution channel, division, sales area, ...</td>
</tr>
<tr>
<td>Financial accounting</td>
<td>Company code, chart of accounts, business area, ...</td>
</tr>
<tr>
<td>Logistics</td>
<td>Purchasing organisation, purchasing group, plant, storage location, ...</td>
</tr>
<tr>
<td>Controlling</td>
<td>Controlling area, cost centre, profit centre, ...</td>
</tr>
<tr>
<td>Human resources</td>
<td>Personnel area, employee group, employee subgroup, ...</td>
</tr>
</tbody>
</table>

General data that is used by all company codes is stored at a client level. This means that data valid for all functional areas needs to be stored only once (eg vendor name and address is stored at the client level whilst payment terms may vary for each company code).

Organisational structures can be used to control access to processing within the organisation. For example, users can be restricted to process documents for their own company code only.

Diagram 1 shows the organisational environment of the company code.
The minimum required organisational structures include the following:

- **An instance** is a single, unique installation of the SAP R/3 software. Generally, separate instances would be used for development, testing, and production.

- **A client** is the highest organisational level within an instance. There is usually one client for an entire organisation. Separate clients would be used for different organisations using the same R/3 installation (as in a service centre situation). Clients have separate unrelated data. The parameters specified at the client level apply to all company codes within that client. Objects in the system can be either client-dependent (i.e., apply only within an individual client) or client-independent (i.e., apply across all clients in an instance).

- **The chart of accounts** sits at the top of the financial accounting structure (a level below client). At least one chart of accounts must be defined. The chart of accounts lists all the G/L account master records, and contains information on the master records that are not company-code-dependent.

- **The company code** represents an independent legal entity for regulatory purposes. The balance sheet and income statement are created at the company code level. Each client may contain a number of companies. Several codes can be set up per client to manage the accounts of independent organisations simultaneously. Each agency would be represented by a separate company code.

Additional organisational structures may also be set up purely for internal reporting purposes. This may include the use of **business areas** which represent an organisational entity that is not a separate legal entity. For example, a company code can be subdivided into several business areas in order to create internal reports on separate subdivisions of the organisation.
The implementation guide (IMG)

The IMG is an online manual that is used to assist in customising SAP R/3. The IMG lists all activities for implementing each SAP module and aids in the documentation and control of the implementation. Diagram 2 illustrates a typical IMG menu screen. The IMG provides the following:

- action plan for customising and implementing the SAP modules;
- an explanation of the concepts that form the basis of the business transactions and the reasons why various steps are required;
- a list of other procedures which need to be performed before implementing the current step;
- a detailed list of the actions that need to be performed and a direct link to the customising transactions required to perform the particular action;
- the ability to document the way in which the system has been implemented and the justification for such implementation; and
- controls over project management, configuration and release.

**Diagram 2: The implementation guide**
**Numbering in SAP**

Every document in the system receives a number which is unique in a company code within a fiscal year. You can specify that numbers are either assigned to documents manually by the user (external number assignment) or a sequential number may be automatically assigned by the system (internal number assignment).

Accounting document number ranges are configured in the system and then allocated to various document/transaction types. The intervals of the number ranges should be unique and should be large enough to support the anticipated volume of transactions.

**Sub-ledger reconciliations**

SAP is a fully integrated system which results in a transaction in one module simultaneously updating other modules in the system. Postings to the accounts receivable and accounts payable sub-ledgers also result in a corresponding entry to a control/reconciliation account in the general ledger on a real-time basis. However, each sub-ledger account (e.g., vendor/customer) can be individually allocated to a nominated reconciliation account. If care is not taken in which reconciliation accounts are allocated, the sub-ledgers may become out of balance with the intended reconciliation accounts in the general ledger. For this reason, it is important that sub-ledger reconciliations are regularly performed, preferably as part of month-end processing. There are various standard reports that can assist in this process.

**Document types and posting keys**

The document type is a two-character alpha-numeric key that identifies documents. Document types are configured in the system and are used to:

- distinguish between the different types of business transactions to be posted (e.g., KR = vendor invoice, SA = general ledger document);
- control which account types may be posted using the document (customer, vendor, general ledger, assets, materials). Account types therefore ensure that transactions (e.g., customer transactions) are posted to the correct general ledger accounts;
- sort documents; and
- assign document numbers.

The posting key is a two-digit code which specifies whether the line item is a debit or credit entry, and the data entry characteristics (field status) for posting.

**Validations and substitutions**

The SAP R/3 system contains many standard edit and validation checks. However, it is also possible to configure additional validation and/or substitution rules that occur at the time of transaction entry to further ensure the integrity of data. Validations are configured in the financial accounting module special ledger (FI-SL).
Validations permit the checking of values and combinations of values as they are input. As data is input, it is checked against the validation rules stored in the system. This allows only valid data to be posted in the system. Validation rules can be created to provide additional validation checks that are not provided by the standard system. An example of a validation may be the validation of company code against business area for document posting.

Substitution is the process of checking entered values (when they are entered into the SAP System) against a user-defined Boolean statement. If the statement is true, the system substitutes specified values into the financial accounting system. The system performs substitutions before validations so that substituted values can also be validated.

**Field status**

Field status refers to the mechanism used to control the data entry characteristics of individual fields and field groups for transactions in the system. The field status can be set to either:

- suppressed (field is hidden and input is not possible);
- required (field must be entered);
- optional (field may be entered); or
- display (field is displayed on the screen but input is not permitted).

Field status can be set separately for different transactions (e.g., creating, changing, displaying) and should be carefully defined to ensure that all data required for processing is entered during data entry. Sensitive fields that should not be modified during data entry should be set to 'suppressed' or 'display only' to prevent changes by the user. Diagram 3 shows a typical field status configuration screen.

The field status can be set in multiple ways including at the account group (a grouping of similar master records for A/P, A/R, G/L), transaction, and company code levels. SAP has set priorities dictating how the field status is applied. The setting of 'suppressed' takes priority over 'display only' which takes priority over 'required entry' which overrides 'optional entry'. SAP interprets the combination of settings and the highest priority setting will be the field status parameter that is adopted by the system to control data entry. It is therefore essential to assess the field status settings at all levels to ensure they accurately reflect the intended design.
**Document change rules**

A document (transaction) can be displayed or changed at any time. ‘Document change rules’ are used to determine which document fields are allowed to be changed and under what circumstances. The system documents all changes to master records and documents via the standard audit trail facilities. Consideration should be given to which fields may be changed and any restrictions that may be placed on the ability to change fields. The ‘document change rules’ should then be appropriately configured via the IMG. Note that changes to standard document change rules may compromise system controls.

Some accounting related fields (account number, amount and posting key) cannot be changed in any documents.

**Reporting and report trees**

Reporting in SAP is performed through the ‘Information system’. There are numerous standard reports which are provided by SAP for each application module. Each of the reports that is intended for use should be attached to the information system ‘report trees’ to enable easy execution of the reports by system users. It may also be necessary to develop custom reports if the organisation’s reporting needs cannot be addressed using the suite of standard reports available.
The reporting tree can assist the user in selecting reports from the information system. The reporting tree is a freely definable structure that can be accessed from within any application by selecting Information system Choose report. The reporting tree is used to collate all reports within an application and sort them by hierarchy. Reports can then be selected from the reporting tree. Most standard reports provide for a variety of selection parameters. A typical report tree is illustrated in diagram 4.

**Diagram 4: SAP report tree**

A useful reporting utility is the use of 'dynamic reporting'. Dynamic reporting allows the user to specify additional selection criteria when executing a report. Selection options can be specified (eg select all transactions greater than $10 000) and additional fields can be included to further refine reporting queries. Dynamic reporting is available via icons titled 'Selection options' and 'Dynamic selections' on the report screen. After selecting 'Dynamic selections' it is possible to select additional fields to use in the query via the 'New field selection' icon.

There are also several tools available for developing custom reports. 'Report writer' is a utility which can be used to generate ABAP/4 reports without requiring any knowledge of the ABAP/4 programming language. 'Report painter' is another utility which allows ABAP/4 reports to be created by selecting the fields and values that should be displayed. 'Report painter' uses a graphical interface and is easier to use than 'Report writer', allowing for simple and flexible report definition and providing direct control over the report layout.
Audit trails and logging

SAP provides an online audit trail for all transactions processed in the system. Each ‘document’ or transaction processed is stored online and it is possible to retrieve information on documents via a number of standard reports and queries in the system. It is possible to review changes made, including the user responsible for effecting the change.

However, there are some deficiencies with the standard SAP reports (‘change records’) as some of these do not provide date-based selection parameters, which makes it difficult to perform an independent review of changes without modifying the standard SAP audit trail report. There are however some reports now available which do provide this facility, and these have been discussed in the relevant sections of the handbook.

Some additional deficiencies of some standard SAP audit trails include:

- Some of the audit trails identify data elements by non-meaningful SAP field names which have been derived from German descriptions. The user of the report therefore needs to understand what these field names represent.
- There is no standard audit trail of corrections to rejected batch input (e.g., interfaces).
- There is no report of warning messages generated as part of batch input processing (which is run in background mode).
- SAP does not provide an exception report of overrides to information defaulted from standing data records.

Introduction to SAP security concepts

Access control within SAP is achieved using the SAP authorization concept. Authorizations are client specific and are based around each individual having an associated user master record for each client that he/she needs to access. SAP security is organised in a hierarchical structure and all components of the hierarchy must be present for security to operate. The general principle behind SAP security is to deny access unless the user is specifically authorised. The elements of SAP security are explained below. The authorisation concept is depicted in diagram 5.
**User master record**

The user master record identifies users and assigns access 'profiles' to the user.

**Profiles**

The profile contains a list of 'authorizations' for business functions. Profiles can be either simple (a collection of authorizations generally providing access to an individual task) or composite (a group of simple profiles which may be grouped to form a job role).

**Authorization**

The authorization provides a nominated level of access to a specific 'authorization object'. Each authorization is a joining of an object (eg vendor company codes) defined within SAP and all valid values the object can take for the user. (eg the permitted company numbers for that user).
**Authorization object**

The authorization object is the foundation of the authorization concept. Objects serve as a template for providing access checks in program code and access rights in the user master records. All objects required to run the SAP system are defined when the system is delivered. It is also possible to define custom objects.

**Profile generator**

Profile generator is the new utility that can be used for implementing SAP R/3 security. It is available and fully supported from release 3.1G of SAP R/3. Profile generator simplifies the approach and reduces the time taken to implement security. It removes the need to work directly with the authorization objects in the system.

Implementation of security using the profile generator involves three main processes:

- the functions/transactions to be performed by a user are selected from the 'Company menu' (which mirrors the SAP menu for the implemented system) and included in the 'activity group'/profile;
- the authorization field values must be maintained for the activity group (e.g., which company codes can be accessed and what activities can be performed). The activity group must be 'generated' before it can be used; and
- the activity group must then be assigned to a user(s).

While the use of profile generator simplifies the approach taken to implementing security, there are still issues associated with security implementation. The security implementation is still open to the possibility of errors and security can still be maintained outside of the profile generator. When profile generator is activated, it is also possible to disable many of the standard system authorization checks.

**Authorization check for transaction start**

SAP introduced a new 'non-application specific' authorization object with release 3.0D called 'Authorization check for transaction start'. This object enables access to be granted to individual transactions via the transaction code. When a user executes a transaction, SAP checks to ensure that the user has the appropriate authorization for the transaction code in order to be able to start the transaction. It should be noted that this will not necessarily enable a user to execute the transaction as a number of additional authorization objects will generally be required to execute a transaction. Reliance solely on authorization checks at the start of transactions is also an invalid approach to securing the system. Instead, the 'Authorization check for transaction start' object should be used to enhance the security already available in the SAP R/3 system. The system will check for this object at the start of each transaction by default unless this is deactivated at a global level. This additional security control should not be deactivated.
# Appendix 2: Glossary of terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABAP/4</td>
<td>Advanced business application programming. The proprietary fourth generation SAP programming language.</td>
</tr>
<tr>
<td>Account assignmen / account determination</td>
<td>A process whereby the G/L accounts to be updated as a result of a transaction are 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>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 either general ledger, customer, vendor, asset, or material. It determines which general ledger accounts can be posted.</td>
</tr>
<tr>
<td>Activation</td>
<td>The process of preparing a profile/authorization for use. When a profile/authorization 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>Activity group</td>
<td>The profile generator equivalent of a simple profile. An activity group is a collection of tasks in the system that are performed for a given user role.</td>
</tr>
<tr>
<td>Application server</td>
<td>The computer which performs the application processing for the SAP system.</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>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Asset master data</td>
<td>A file containing information about the agency's assets including description, location, acquisition cost and accumulated depreciation. An asset master record must be established for each asset the agency purchases or owns.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Defines an access right for an individual authorization object (ie. assigns values for the fields in the object). Authorizations are grouped together to form profiles which are in turn assigned to users.</td>
</tr>
<tr>
<td>Authorization group</td>
<td>An authorization group is a group that can be defined to restrict access to executing/maintaining programs in SAP. An authorization group can be allocated for each program and users can then be given access to perform functions for specific authorization groups only.</td>
</tr>
<tr>
<td>Authorization object</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 authorization objects these are referred to as authorizations.</td>
</tr>
<tr>
<td>Authorizations infosystem</td>
<td>A menu structure which allows users to easily select reports which relate to security. Accessed via transaction SUIM.</td>
</tr>
<tr>
<td>Basis</td>
<td>The core module of the SAP system. The basis module is used for managing security, customising the system, and performing general system administration tasks.</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>Baseline date</td>
<td>The date which is used (in conjunction with the terms of payment) to determine when payment should be made.</td>
</tr>
<tr>
<td>Batch input</td>
<td>Data which forms the basis for batch (background) processing.</td>
</tr>
<tr>
<td>Blocked stock</td>
<td>Stock which has not been ‘released’ for use by the organisation. Stock may be receipted into blocked stock if for example it is subject to inspection or is in an unsatisfactory condition. Care should be exercised when using blocked stock as goods receipted into blocked stock will not be valued in the general ledger.</td>
</tr>
<tr>
<td>Business area</td>
<td>An organisational structure within SAP which can be used for internal reporting purposes (eg administration). Internal financial reports can be prepared for a business area but these do not satisfy all external reporting requirements.</td>
</tr>
</tbody>
</table>
Appendix 2

Business continuity plan  A plan which outlines what steps are to be taken to continue the business in the event of a disaster. This plan would outline backup sites, systems or manual procedures which would need to be implemented to allow the business to continue its normal operations.

C

Change control process  A process whereby changes to programs and other objects in the system are managed. Refer CTS.

Clearing  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.

Client  The highest level in the SAP organisational structure. The client would usually represent the entire organisation or a group of companies. Individual organisations or subsidiaries are represented by separate 'company codes' (or separate legal entities) within the client.

Client copy  The act of copying objects from one client to another client. This can be done within the one SAP environment eg development, or from one SAP environment to another, eg from development to test.

Client-independent table  Tables may be client-independent which means that if it is maintained in one client, the changes will affect all clients within an instance.

Client/server  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).

Composite profile  A profile which consists of a collection of simple profiles. A composite profile generally groups related tasks to form a job role.

Configuration  Refer to 'Customising'.

Configuration objects  Areas of the system which can be configured ie. customised. Generally these will be in the form of entries in a table.

Controlling  The controlling (CO) module is used for management reporting.

CTS  Correction and transport system. The mechanism used for moving objects (programs, tables, configuration, data) between SAP environments.

CTS tables  The correction and transport system requires configuration to be set up to enable it to work. This configuration is stored in the CTS tables.

Customising  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 organisation before it can be used.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data dictionary</td>
<td>The data dictionary is used to store information centrally about the organisation's data. It controls the relationships between the data and how the data is used in programs and screens.</td>
</tr>
<tr>
<td>Database server</td>
<td>The computer which contains the SAP database and performs the database management functions.</td>
</tr>
<tr>
<td>DBMS</td>
<td>Database management system. Software which is used to manage the SAP database (eg Oracle, Informix).</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>Debug</td>
<td>The process of working through a program line by line to determine where an error is occurring.</td>
</tr>
<tr>
<td>Development environment</td>
<td>The environment of the SAP system in which system support staff make changes to programs and other objects in the system. Refer also to test environment and production environment.</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>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 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 date</td>
<td>The date of an original source document which is being processed in SAP.</td>
</tr>
<tr>
<td>Document type</td>
<td>Determines the type of transaction being processed. Document type controls the number ranges used for posting and also determines what type of account can be posted for a given transaction (eg a vendor document type can only be posted against vendor accounts).</td>
</tr>
</tbody>
</table>
EDI
Electronic data interchange. The process of exchanging data (e.g., sales orders) via electronic communications channels. SAP has special features which permit the processing of EDI transactions.

ERS
Evaluated receipts settlement. The process by which suppliers are paid on the receipt of goods without the need for a separate invoice to be received.

Exit
See User exit

Features
Objects used in the HR module to control various operations in the system (e.g., defining default values such as the default payroll payment methods).

Field status
Refers to the data entry option of an individual field. These can generally be set as one of the following:

- required/mandatory - field must have a valid data entry;
- optional - field may have data entry or may be left blank;
- display only - field is displayed on the screen but data may not be entered; or
- suppressed - field is not displayed on the screen therefore data may not be entered.

FI
Financial accounting module. This module consists of several components including general ledger, accounts receivable, accounts payable, assets accounting, legal consolidation and special ledger.

GR/IR clearing account
A clearing account in the general ledger that represents the timing difference between the receipt of goods and the processing of an invoice.

GR/IR control indicators
Fields which are used during the creation of a purchase order. These include:

- GR - goods receipt is required;
- IR - invoice receipt is required;
- GR based invoice verification - goods receipt is required to be processed before invoice receipt; and
- Unval GR - unvaluated goods receipt.

These fields can be made mandatory (see field status) to control the invoice matching process.

GUI
Graphical user interface - the interface that is presented to the user (i.e., screen design and layout).
Held documents | Documents which have been partially entered but are unable to be completed for some reason (eg missing a key element of information). The document may be ‘held’ in the system which results in the document being saved without updating the general ledger. Held documents should be used with caution as they can only be identified and further processed by the user who entered the original document.

IMG/implementation guide | The implementation guide (IMG) is an online manual that is used to assist in customising SAP. The IMG lists all activities for implementing each SAP module.

Info record | 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.

Infosystem | A collection of reports grouped by application area within SAP (eg accounts payable infosystem).

Infotype | Changes are performed on HR master data through groups of information called infotypes (eg taxation information). Infotypes are created for each master record as applicable.

Instance | 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.

Instance profile | A file containing configuration parameters for the application server.

Integration testing | The process of testing a component of system functionality to assess the effects on the system in its entirety (ie assessing the effect on other modules in the system).

Internet firewall | A security system designed to prevent unauthorised access to the organisation's systems by external parties via the internet.

Item category | Refers to configuration settings in the system which control the processing of purchasing transactions. The item category settings can be used to determine whether a goods receipt and invoice are necessary and whether the user can change this within the purchasing documents.
<p>| <strong>L</strong> | Legacy system | 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. |
| <strong>M</strong> | Matchcode | An SAP mechanism that allows the user to search for database records (e.g., vendor master files) by entering some search criteria. A list is then displayed which matches the search criteria and the user can select the appropriate record from the list. |
| | Material master data | A file containing information about the materials (goods) that the agency is purchasing. SAP can be set up to automatically suggest the appropriate vendor to supply a given material. |
| | Materials requirement planning (MRP) | 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. |
| | Movement type | A three-digit code used by SAP to determine the nature of a goods movement transaction (e.g., goods receipt, goods issue, transfer of goods). It also determines which general ledger accounts are updated as part of the transaction. |
| | Moving average price | A material price that is updated after each purchasing transaction by determining the overall average price of the purchased material. |
| <strong>N</strong> | Number range | 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. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-time vendor</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>Operating system</td>
<td>The software used to control the operation of the computer system (e.g., UNIX, Windows NT).</td>
</tr>
<tr>
<td>Organisational assignment</td>
<td>The act of allocating an employee to a position within the organisation.</td>
</tr>
<tr>
<td>OSS</td>
<td>Online support service. 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 organisation's system via the OSS utility to provide analysis services.</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>Parked documents</td>
<td>Documents which have been partially entered but are unable to be completed for some reason (e.g., missing a key element of information). The document may be 'parked' in the system which results in the document being saved without updating the general ledger. Parked documents may then be 'posted' (updated to the general ledger) by another user with appropriate authority.</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>Payment methods</td>
<td>The method of payment (e.g., cheque, electronic funds transfer).</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 organisation. 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>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Presentation server</td>
<td>Another term used to describe the ‘client’ in the client/server model. This is usually the PC on the user’s desk which is used to perform the presentation tasks (ie display the application to the user and receive input from the user).</td>
</tr>
<tr>
<td>Production environment</td>
<td>The ‘live’ SAP system in which the agency actually performs all of its processing. Refer also to development environment and test environment.</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>Profile generator</td>
<td>A tool used to automate the creation of profiles based on menu functions. Refer Appendix 1.</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 value keys</td>
<td>Used to assign a number of default settings (eg delivery tolerances) to material master records.</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 (eg 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>Recurring documents</td>
<td>Transactions which are processed on a frequent/recurring basis (eg rent or lease payments). The system can be set up to process these transactions automatically on a frequency/schedule determined by the user.</td>
</tr>
<tr>
<td>Recurring entry program</td>
<td>The program used to process recurring invoices/documents automatically.</td>
</tr>
<tr>
<td>Release</td>
<td>The version of SAP (eg SAP R/3 release 3.1H). There are usually two to three new releases of SAP produced each year.</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</td>
<td>A mechanism used to control the electronic authorisation of purchase requisitions/purchase orders based on the delegation levels/approval sequences defined for your organisation.</td>
</tr>
<tr>
<td>Repair</td>
<td>A correction/modification made to an SAP object.</td>
</tr>
<tr>
<td>RFQ</td>
<td>Request for quotation - requests for potential vendors to submit a quotation.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SAP environments</td>
<td>SAP environments generally refer to the breakdown between the development, test and production instances of a SAP installation. Programs and other objects are moved between these environments via the correction and transport system.</td>
</tr>
<tr>
<td>SAP*</td>
<td>SAP* 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>Scheduling agreement</td>
<td>A contract for supply of goods according to a schedule containing precisely defined dates on which deliveries are to be made.</td>
</tr>
<tr>
<td>Search term</td>
<td>A field contained in vendor/customer master records which can be used to facilitate searching for vendors/customers (eg the search term field may be used to store an abbreviated search name for the vendor/customer).</td>
</tr>
<tr>
<td>Session</td>
<td>An 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>Simple profile</td>
<td>A collection of authorizations which have been grouped together to be allocated to a user (to assign access capabilities). A simple profile generally provides the access required for a single task.</td>
</tr>
<tr>
<td>Source list</td>
<td>A list containing the possible sources of supply (ie 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>Spool management</td>
<td>The process of managing printer functions within SAP.</td>
</tr>
<tr>
<td>Standard profiles</td>
<td>SAP is delivered with a set of standard profiles (eg SAP_ALL). These should generally not be used in a production environment. Instead, custom profiles should be built, possibly with the profile generator. These custom profiles should comply with SAP naming conventions (usually starting with Z).</td>
</tr>
<tr>
<td>Storage location</td>
<td>An organisational structure in SAP used to represent a storage area/delivery point. Storage location may be a subdivision of plant.</td>
</tr>
</tbody>
</table>
Super user
A system user-id with powerful (often unlimited) access privileges.

System profile parameter
Refer ‘Instance profile’.

System tables
Tables which contain data specifically relevant to system settings (eg correction and transport system tables).

Table
A structure used within SAP to store transaction data, basic commercial data, configuration and system parameters, organisational structure data, and calculation rules.

Table class
A way of grouping tables. Tables can be allocated to table classes to provide security. User access can be confined to specified table classes.

Table maintenance
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.

Test environment
The environment of the SAP system in which system support staff and other users test changes to programs and other objects in the system. Refer also to development environment and production environment.

Transaction
Various functions within SAP are referred to as transactions. Most functions can be invoked by a four character transaction code.

Transport
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.

Unit testing
The process of testing some SAP functionality to ensure that is operates as intended but without consideration of the effect of this function on other modules in the system (eg testing that an asset can be acquired but without testing that the general ledger is accurately updated).

User acceptance testing
Refers to the process of obtaining user acceptance of the designed system through comprehensive testing of all system functionality. Users should be involved in testing all components of the system and approving the design prior to implementation. This should assist in highlighting whether the system meets the needs of the end users.

User exit
A point in an SAP program which enables the activation of a custom program to perform a function that is not performed by the standard program.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 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>Vendor master data</td>
<td>A file containing information about the agency's vendors including name and address, terms of payment, payment information (eg 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>Wage types (HR)</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>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>An SAP utility that can be used to control the time and logical sequence in which work items are processed (eg 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>
Index

A

ABAP programs ........................................ 144,150,156,157,165,193
access control checks .................................. 155
access requests ......................................... 147
access rights ........................................... 124,152
access security ......................................... 5,152,160
account assignment .................................... 15,16,193
account group ......................................... 73,79,193
account number ...................................... 55
account type ........................................... 91,193
accounting data ....................................... 42,52,54,83,86
accounting periods .................................... 83,87,112
accounts marked for deletion ......................... 86
accounts payable module .............................. 12,50-60,61,71
subledger ............................................. 44,46,57,63,65,78
accounts receivable ................................... 71,82,91
duplicates ............................................. 83,87
subledger ............................................. 78
accrual entries ......................................... 82
activation ................................................ 193
administrator ......................................... 151
activity based costing ................................ 108
activity groups ........................................ 150,191,193
alternate payees ....................................... 21,23
analysis of table log database report ............... 159,166,168
ANAO ................................................... see Australian National Audit Office
annual leave ........................................... 131,132
application server ..................................... 193
approval procedures ................................ 12,13,60
archiving ................................................. 157
asset acquisition ...................................... 93-7
asset acquisition report ................................ 97
asset classes ......................................... 94,95,96,106,193
asset depreciation ................................... see depreciation
asset ledgers ........................................... 93,102
asset master record .................................. 93,94,95-7,102,194
redundant screens .................................... 96
asset numbers ........................................ 96
asset retirements ...................................... 98,100
assets retirements report ............................. 101
asset transfers ........................................ 98-101
asset transfers report ................................. 101
assets accounting (FI-AA) module .................. 2,71,92
see also low value assets
changes to ............................................... 95
end-of-month procedures ......................... 104
physical count ......................................... 100
segregation of duties ................................. 97,101,105
transaction types ..................................... 100
ATO notification report .............................. 136
audit techniques ....................................... 4,189
Australian National Audit Office .................... 4
handbook ............................................... 2
Financial Statement Audit .......................... 4
internet address ....................................... 2
authorization administrator ....................... 151
authorization checks ................................ 150,151,157,191
authorization concept ................................ 7,189-92,194
authorization groups ................................ 29,53,156,194
authorization objects ................................ 19,25,60,68,191,194
ABAP/4 Program run checks ......................... 157
accounting document: account authorization for customers ..................... 91
accounting document: authorization for account types ........................ 91
authorization for transaction start ................ 161,191
balance sheet: general maintenance authorization ................................ 91
check management: action auth for company codes ................................ 68
customer: application authorization ................ 81
G/L Account: Account authorization ............. 75
G/L account: authorization for charts of accounts/ company code ............ 75
HR: master data ..................................... 124
HR: master data—personnel number check ........ 124
HR: master data extended check .................. 124
system administration function .................. 157
table maintenance ................................... 159
workbench organizer and transport system ...... 157,168
authorization procedures ......................... 17,18,150
authorizations infosystem report tree ............ 194

B

background processing ................................ 194
backup and recovery procedures ................. 140,141,148
balance sheet accounts ............................... 73
balance sheet supplement—open item analysis .......................... 90
bank account numbers ................................ 121,134
bank accounts ........................................63,68,91,135
bank deposit summary report ..................134,135
bank reconciliation .................................65
bank transfers .......................................61
baseline data .......................................194

Basis component (BC) module ..............2,137–80,194
batch input ........................................194

batch input: display logs ......................175
batch input error correction .................170
batch input session ..............................171
batch interface ....................................86
batch processing ..................................157
duplicate batch files .........................171

batch session .....................................105
best practice ....................................see also better practice procedures .iii,3,6-7,17
better practice .....................................1
blocked stock .....................................31,35,194
business area .....................................182,183,194
business continuity plan .....................148,195
business processes .............................17,140

business software  see SAP R/3

C

calculation key ....................................194
career planning ...................................116
cash discounts ....................................63
CEMETEX tape ...................................130,134
change control function .......................139
change control procedures ...................164,165
change control process .......................163–68,195

change documents .............................59,161
change options ...................................164
changes, unauthorised .........................170

changes to master records ....................97
chart of accounts ............................72,73,182,183
company code level ............................73

check lists ......................................128,146

check passwords of SAP* .....................161

cheques ..........................................61
‘lots’ ..............................................65
manual .............................................62,64,66,67
printing errors ....................................65

clearing ..........................................64,195
clearing accounts ................................111
client copy .......................................195
client-dependent object .......................164
client-independent table .....................195

client/server ......................................195

clients .............................................4,164,183,195
code combinations ..............................111

Commonwealth Public Sector agencies . see government agencies

compact document journal .....................54,89
company codes .................................56,72,73,76,91,182,183

comparison tool ................................161
configuration elements ......................165,166
composite profile ...............................195

correction and transport system (CTS) . see customising
configuration objects .........................195
contracts ...........................................15
contracts source list ..........................see source list
control indicators ..............................111
control issues ....................................5

Control Record ................................127,129
Controlling (CO) module .....................2,107–14,182,195
central interface ................................108,112
master records ....................................112
order and project accounting .............108
product costing ................................108
profit centre accounting ......................108
profitability analysis .........................108

conversion dependencies .....................178
conversion planning .........................178–79
correction and transport system (CTS) . see customising
tables .............................................164,166,167,168,195

cost allocations ................................109
cost centre accounting .......................108
cost centres ......................................104,111
security .........................................113
cost planning ....................................116
country specific settings .....................121
credit control area .............................183
credit management change display .......81
credit notes ....................................42,54

cross-application matters ....................6,137,139
CTS .............................................see correction and transport system
currency ........................................15,54,78

see also foreign currency
current active users .........................161
custom transactions .........................150,155
custom validations ................................88
customer account balances ..................89
customer changes (accounting) ............75
customer invoices ...........................see under invoices
customer list .................................see under invoices
customer master data .................................................... 76-81,86
changes ................................................................. 80
duplicate records ..................................................... 78
segregated duties ....................................................... 81
tolerances .............................................................. 88
customer pricing procedure ....................................... 78
customers with missing credit data .............................. 81
customising ............................................................ 195
data administration ............................................. 140,147
data cleansing ......................................................... 176,178
data conversion ......................................................... 4,176-80
strategy ................................................................. 177
data dictionary ......................................................... 159,196
data ownership ......................................................... 141,147
Database Management System (DBMS) ............. 4,196
database server ......................................................... 196
DBMS see Database Management System
DDIC ........................................................................ 196
debug access .......................................................... 157,196
delegation structures ................................................. 19
deliveries ................................................................. see also returned deliveries
delivery complete indicator ................................... 35,37
partial ................................................................. 33,34
delivery tolerances .................................................. 14,15,31,34-5
depreciation .............................................................. 100,102-6
keys ................................................................. 102,103-4
depreciation report ................................................... 105
design documentation .............................................. 144
desktop PC .............................................................. 4
developer access rights ........................................... 150,165
development environment ....................................... 196
development objects ............................................... 196
directory of unposted assets .................................. 97
disaster recovery plan (DRP) ..................................... 148,196
discount rates ........................................................... 42,66
discounts ................................................................. 55
see also cash discounts
display info record changes .................................. 19
display of bank changes ........................................... 25
display of changed documents .................................. 90
display of customer changes .................................... 81
display of vendor changes ....................................... 25
distribution channels ............................................... 182
divisions ................................................................. 182
document .............................................................. 196
change rules ......................................................... 187
date ................................................................. 100,196
header ................................................................. 187
number .............................................................. 54,56,101,185
reconciliation ......................................................... 90,178
reversals ............................................................ 54,56,66,88,111
types ................................................................. 171,185,196
double verification principle ................................... 120
down payments ....................................................... 66
downloading to diskette ......................................... 173
dynamic reporting ................................................... 188
EDIC (electronic data interchange) ...................... 197
efficiency ............................................................... iii
electronic approval ................................................... 12,13
electronic authorisation ........................................... 17
emergency access procedures ............................. 155
emergency change procedures ............................ 165
emergency repairs .................................................. 167
employee group ..................................................... 182
employee pay details (payroll result) report ........ 135
employee remuneration information screen ........ 126,128
employees .............................................................. 116
benefits .............................................................. 132
changes to data ......................................................... 118,120
events ................................................................. 120
hiring ................................................................. 117
personal data ........................................................ 121
standing data ........................................................ 117
termination of see termination processing
ERS see evaluated receipts settlement
evaluated receipts settlement (ERS) .................... 24,39,41,42,197
log ................................................................. 48
exception report .................................................... 18,35,48,53,54,55,59,123,134,189
exchange rates ....................................................... 44,55,78
exit see user exit ..................................................... 169,173
extended systems see also extended systems
F

features ...........................................197

FI see financial accounting

FI document: list of update termination ........89

field groups .......................................29

field status ..................................15,73,95,186-87,197

company code level ..............................186

financial accounting (FI) module ...............2,50,52,69-105,182,197

clearing program ................................44

held documents ..................................85

maintenance .....................................75

restricted access ................................91

financial accounting comparative analysis
report ................................................174,175

financial assets ...................................3

financial records ...................................3

financial statement audits ........................4

financial statements .............................90

company code level .............................183

fixed assets ......................................92,94,95

control accounts ................................104

physical count of ................................95

sub-ledger ........................................95,100,104

foreign country transactions .....................44,57,89

GR/IR clearing account ...........................197

GR/IR control indicators .........................197

Graphical User Interface (GUI) ...................4

H

hand-coded username ............................172,173

‘held’ username .................................54,86,87,198

‘hot spots’ documents.............................6

asset master records ............................94

asset transfers ...................................99

change controls ..................................164

cost allocations ..................................110

depreciation areas ...............................103

goods receipts ....................................31

in financial accounting ...........................83

in material transactions ...........................27

invoice verification ..............................40,51

payee ...............................................21

payments .........................................62,126

purchasing ........................................14

security ............................................150

human resources (HR) module ...............2,115-36

confidentiality ....................................118

fast entry facility .................................122

features ............................................198

master data maintenance ........................119-24

segregation of functions .........................124

G

general journals .................................82

G/L ....................................................see general ledger

general ledger (G/L) .............................16,33,44,71,82-91

balances ..........................................84,85,87

journals ............................................86

master data .........................................72,73,74,85

month-end processing ............................87

processing procedures ............................87,91

general ledger account balances ...............90

general ledger account changes .................75

general ledger (G/L) accounts ....................16,36

adjustment accounts ............................111

changes ............................................74

duplicates ..........................................73

payroll ..............................................128

profit and loss accounts ........................111

sample accounts ....................................73

general ledger journals ........................see journal processing

goods receipts ....................................12,16,17,30-8,44,93

processing .........................................32-3,45

quantity variance ................................45

return/write off transactions ....................31

reversal entries ...................................35

unmatched .........................................41,48

government agencies ............................iii,1,105

organisational units .............................143

GR/IR clearing account ...........................197

GR/IR control indicators .........................197

Graphical User Interface (GUI) ...................4

I

IMG ..................................................see Implementation Guide

Implementation Guide .............................144,184,198

implementation partners ........................3

info record ........................................198

information availability ........................iii

confidentiality ....................................iii

integrity ............................................iii

information records .............................15

display of changes ...............................19

Information Technology (IT) departments .......5,146

security plans .....................................see security plans

infrastructures ....................................198

infotypes ...........................................116,118,122,198

changes to 119,123,128

deactivation .......................................121

objects on loan .................................122

security of ........................................124

instance ...........................................see SAP R/3 - instance

instance profile ..................................198

integration switches .............................118,121

integration testing ...............................198

interfaces .........................................169-75

Internal Audit ....................................3

internal control mechanisms ........................iii,1
parked documents ................................. 84,85,86,87,200
passwords ......................................... 153,158
default system ................................. 153,155,158
prohibited ....................................... 154
patches ........................................... 200
payment exception list ......................... 65,68
payment list ...................................... 68
payment methods ................................ 200
payment processing ............................. 12,61-8
payment program ................................ 71
open items ........................................ 61
reports ............................................ 65
payment proposal list ............................. 63,65,68
payment release procedures ..................... 60
payment terms .................................... 15,24,42,66,78
payments ......................................... see also down payments
authorised ....................................... 67
blocked ........................................... 66
blocking reasons ............................... 62,65
data entry ....................................... 63,126
default payment method ......................... 129
differences ....................................... 60
flagged ........................................... 66
minimum payment accounts ................. 129
minimum values ................................ 62
prompt payment discounts ...................... 12,61
recurring ........................................ 129
residual .......................................... 60
tolerances ....................................... 60
unauthorised ..................................... 12
payment run ...................................... 12,51,64,66,68
payroll accounting .............................. 121
authorisations .................................. 133
default payment method ......................... 126,129
payroll areas ..................................... 127
period ............................................ 127
retrospective ..................................... 126
run to run reconciliation report ............... 129
payroll adjustments ............................. 128
payroll calculations ............................. 125-36
payroll data ...................................... 120
control record .................................. 127
PD authority profiles ........................... 124
payroll exceptions report ....................... 133,135
payroll history (payroll payment)
report .............................................. 135
payroll information system ...................... 135
payroll payment .................................. 125-36
see also CEMTEX tape
payroll period ................................... 126,127,129
payroll program ................................. 116,117,130
exceptions report ............................... 116,117,130
retroactive accounting ......................... 129
retrospective adjustments ...................... 126,127
status record .................................... 120,122,126,134
subgroups ........................................ 122
payroll staff ..................................... 124
payroll totals .................................... 127
period ending closing procedures .............. 89
personnel administration (HR-PA) .............. 116,121
personnel calculation rules ..................... 128
checking function ................................ 118
personnel numbers .............................. 119,121,124,130
personnel officers ............................... 124
personnel planning and development (HR-PD) 116
PIR .................................................. see purchasing info records
plant ................................................. 200
position-based security ......................... 124
positive acknowledgment scheme ............ 172
post code data .................................... 121
post-implementation review .................... 145
posting totals .................................... 89
postings ............................................ 36,82
automatic ....................................... 46,65,84,87
blocked ........................................... 88
controlling module ............................. 111
date ............................................... 54,56,101,200
key (debit or credit code) ....................... 55,185,200
park and post functionality ..................... 53,84
period ............................................ 56,66,87,91,103,104
transactions ..................................... 109,110
year-end ......................................... 88
presentation server .............................. 201
price change for vendor’s contracts ............ 25
price change for vendor’s info records ........ 25
price change for vendor’s scheduling agreement 25
price list type .................................... 78
primary cost elements .......................... 112
procurement cycle .............................. 11,92
conflicting duties .............................. 25,60,68
procurement process ........................... 11
production environment ....................... 150,201
profile ............................................ 201
profile generator ............................... 151,154,191,201
profit and loss accounts ....................... 73
profit centres .................................. 108,111
project management ........................... 3-4
Protective Security Coordination Centre ....... iii
Protective Security Manual ...................... iii
public sector agencies ........................ see
government agencies
purchase order processing ...................... 11,18
purchase orders ........................................... 12,13,15,45
blocked .................................................. 15
conversion ............................................. 177,179
duplicate ................................................ 16
numbers .................................................. 33,36
price history ........................................... 19
sensitive information ................................... 15
unreleased ............................................. 18
warning .................................................. 16
purchase requisitions .................................. 11,12,13
approval of ........................................... 17
purchasing data ........................................ 15
purchasing documents ................................ 15,16,17,201
see also purchase order; purchase requisition
automatic generation ................................... 28
changes ................................................... 19
restricting access ....................................... 19
purchasing documents by vendor .................. 19
purchasing group ....................................... 16,182,183
purchasing info records (PIR) ......................... 24
changes ................................................... 24
purchasing master data ................................ 16
purchasing value keys .................................. 31,35,201
report writer utility ..................................... 113,188
reporting tree .......................................... 187-88
reports ................................................... 19,25,38,187-88
controlling ............................................. 113
exception reports ...................................... 55,59
financial Accounting ................................... 75,90
infotypes ............................................... 123
on asset transfers ....................................... 101
on invoices ........................................... 59
payment program ..................................... 68
payroll processing ..................................... 135
security function ...................................... 161
to management ....................................... 108,109
requirements planning ................................ 11
see also materials requirement planning
requisition stage ........................................ 12
requisitions ........................................... 13
restricted access ....................................... 19,91,155,156
returned deliveries ..................................... 35,36
revalue open accounts .................................. 89
reversing documents .................................. 91
RFQ (request for quotation) .......................... 201
risk assessment ......................................... 11
risks ....................................................... 6
in material transactions ................................ 27
mitigation of ........................................... 3
purchasing ............................................. 14
RSBDCSUB ........................................... 135
run to run reconciliation report Australia .......... 135

Q

qualifications ........................................... 116
quality assurance (QA) procedures ................. 166
quotations ............................................. 13

R

real-time .................................................. 201
receipt of goods and services ....................... 30,34
documents ............................................ 36,38
reconciliation
accounts .............................................. 44,57,73,78,174,201
FI/CO ...................................................... 111
ledger .................................................... 112
recruitment ............................................. 116
recurring documents ................................ 201
recurring entry documents .......................... 83,85,88,90
recurring entry program (RSBDCSUB) ............ 54,57,91,201
recurring journals ..................................... 86,88
release ................................................... 201
release codes .......................................... 19
and group (purchasing) .............................. 19
in purchase requisitions .............................. 19
release indicators ..................................... 14
release procedures ................................... 17,201
release strategies ..................................... 14,201
repair ..................................................... 201
report painter utility .................................. 113,156,188
report writer utility ..................................... 113,188
reporting tree .......................................... 187-88
reports ................................................... 19,25,38,187-88
controlling ............................................. 113
exception reports ...................................... 55,59
financial Accounting ................................... 75,90
infotypes ............................................... 123
on asset transfers ....................................... 101
on invoices ........................................... 59
payment program ..................................... 68
payroll processing ..................................... 135
security function ...................................... 161
to management ....................................... 108,109
requirements planning ................................ 11
see also materials requirement planning
requisition stage ....................................... 12
requisitions ........................................... 13
restricted access ....................................... 19,91,155,156
returned deliveries ..................................... 35,36
revalue open accounts .................................. 89
reversing documents .................................. 91
RFQ (request for quotation) .......................... 201
risk assessment ......................................... 11
risks ....................................................... 6
in material transactions ................................ 27
mitigation of ........................................... 3
purchasing ............................................. 14
RSBDCSUB ........................................... 135
run to run reconciliation report Australia .......... 135

S

sales .......................................................... 98
sales and distribution module ....................... 76,78,82,182
sales tax ................................................... 46
SAP
administrator .......................................... 167
organisational structure ................................ 143
public sector template ................................... 1
security .................................................. 149-62
SAP* ...................................................... 150,153,158,202
SAP Australia ........................................... 1,3
SAP R/3
application modules ................................... 1
see also modules
access profiles ......................................... 144,152
background session ................................... 171
calculation rules ....................................... 5
concepts .................................................. 7,182-92
conventions ............................................ 155
custom development classes ......................... 167
data administration and ownership ................. 147
design phase .......................................... 5,141
development functions ................................ 156
environment ........................................... 4,140,165,202
implementation ....................................... 135,140,141,184
instance .................................................. 183


SAP R/3 cont.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>interfaces</td>
<td>169</td>
</tr>
<tr>
<td>modifications</td>
<td>144,167</td>
</tr>
<tr>
<td>module overview</td>
<td>2</td>
</tr>
<tr>
<td>override capabilities</td>
<td>5</td>
</tr>
<tr>
<td>payroll system</td>
<td>129</td>
</tr>
<tr>
<td>release 3.1H</td>
<td>2</td>
</tr>
<tr>
<td>review</td>
<td>4</td>
</tr>
<tr>
<td>sequence checking</td>
<td>171</td>
</tr>
<tr>
<td>standard profiles</td>
<td>156</td>
</tr>
<tr>
<td>standard users</td>
<td>141</td>
</tr>
<tr>
<td>system profile parameters</td>
<td>150</td>
</tr>
<tr>
<td>three way match</td>
<td>66</td>
</tr>
<tr>
<td>validation rules and tables</td>
<td>5,179</td>
</tr>
<tr>
<td>workflow</td>
<td>12,60</td>
</tr>
<tr>
<td>SAPRouter</td>
<td>142,202</td>
</tr>
<tr>
<td>SAP system log</td>
<td>162</td>
</tr>
<tr>
<td>scheduling agreement</td>
<td>202</td>
</tr>
<tr>
<td>scrapping</td>
<td>98</td>
</tr>
<tr>
<td>search term</td>
<td>24,202</td>
</tr>
<tr>
<td>security administration</td>
<td>149,150,151-53</td>
</tr>
<tr>
<td>security administrators</td>
<td>151</td>
</tr>
<tr>
<td>security issues</td>
<td>4,5,60,141,146,149</td>
</tr>
<tr>
<td>external security systems</td>
<td>151</td>
</tr>
<tr>
<td>guidelines</td>
<td>155,189</td>
</tr>
<tr>
<td>global security parameters</td>
<td>149,153</td>
</tr>
<tr>
<td>security plans</td>
<td>III,140,146</td>
</tr>
<tr>
<td>implementation</td>
<td>160</td>
</tr>
<tr>
<td>security policy</td>
<td>146,155</td>
</tr>
<tr>
<td>SECUDE</td>
<td>151</td>
</tr>
<tr>
<td>server operating system</td>
<td>4</td>
</tr>
<tr>
<td>service entry sheet</td>
<td>32,33</td>
</tr>
<tr>
<td>services</td>
<td>16,32,33</td>
</tr>
<tr>
<td>unplanned</td>
<td>33</td>
</tr>
<tr>
<td>session</td>
<td>202</td>
</tr>
<tr>
<td>SGC</td>
<td>see Superannuation Guarantee Charge</td>
</tr>
<tr>
<td>simple profile</td>
<td>202</td>
</tr>
<tr>
<td>source list</td>
<td>11,13,15,16,28,202</td>
</tr>
<tr>
<td>SGC month employee report</td>
<td>136</td>
</tr>
<tr>
<td>special ledger</td>
<td>109,202</td>
</tr>
<tr>
<td>reporting system</td>
<td>71</td>
</tr>
<tr>
<td>spool management</td>
<td>202</td>
</tr>
<tr>
<td>staff retention</td>
<td>5</td>
</tr>
<tr>
<td>standard profiles</td>
<td>202</td>
</tr>
<tr>
<td>stochastic blocking</td>
<td>57</td>
</tr>
<tr>
<td>stock balance</td>
<td>35</td>
</tr>
<tr>
<td>stock levels</td>
<td>29</td>
</tr>
<tr>
<td>stocktakes</td>
<td>32</td>
</tr>
<tr>
<td>storage location</td>
<td>182,183,202</td>
</tr>
<tr>
<td>data</td>
<td>35</td>
</tr>
<tr>
<td>subledger reconciliations</td>
<td>185</td>
</tr>
<tr>
<td>substitution</td>
<td>186</td>
</tr>
<tr>
<td>succession planning</td>
<td>116</td>
</tr>
<tr>
<td>super users</td>
<td>158,203</td>
</tr>
<tr>
<td>superannuation calculation rules</td>
<td></td>
</tr>
<tr>
<td>superannuation employee report</td>
<td>136</td>
</tr>
<tr>
<td>superannuation fund report</td>
<td></td>
</tr>
<tr>
<td>Superannuation Guarantee Charge</td>
<td>128,136</td>
</tr>
<tr>
<td>superannuation liability</td>
<td></td>
</tr>
<tr>
<td>supplier invoice data</td>
<td>see accounts payable subledger</td>
</tr>
<tr>
<td>system administration functions</td>
<td>139</td>
</tr>
<tr>
<td>system customising tables</td>
<td>168</td>
</tr>
<tr>
<td>system documentation</td>
<td>144</td>
</tr>
<tr>
<td>system profile parameter</td>
<td>203</td>
</tr>
<tr>
<td>system security functions</td>
<td>139,153,156</td>
</tr>
<tr>
<td>system security plans</td>
<td>see security plans</td>
</tr>
<tr>
<td>system tables</td>
<td>159,203</td>
</tr>
</tbody>
</table>

T

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>table</td>
<td>203</td>
</tr>
<tr>
<td>table class</td>
<td>203</td>
</tr>
<tr>
<td>table maintenance functions</td>
<td>150,159,203</td>
</tr>
<tr>
<td>client-independent tables</td>
<td>159</td>
</tr>
<tr>
<td>CTS tables</td>
<td>164</td>
</tr>
<tr>
<td>'table class' assignment</td>
<td>159</td>
</tr>
<tr>
<td>tax</td>
<td>42,45,55,105</td>
</tr>
<tr>
<td>balance sheet</td>
<td>105</td>
</tr>
<tr>
<td>scale</td>
<td>130</td>
</tr>
<tr>
<td>temporary staff</td>
<td>152</td>
</tr>
<tr>
<td>tender evaluation process</td>
<td>11</td>
</tr>
<tr>
<td>termination processing</td>
<td>121,130</td>
</tr>
<tr>
<td>terms of payment</td>
<td>55</td>
</tr>
<tr>
<td>test environment</td>
<td>165,203</td>
</tr>
<tr>
<td>testing procedures</td>
<td>166</td>
</tr>
<tr>
<td>time-out facilities</td>
<td>153</td>
</tr>
<tr>
<td>tolerances</td>
<td>see delivery tolerances</td>
</tr>
<tr>
<td>training</td>
<td>116,145</td>
</tr>
<tr>
<td>transaction access lists</td>
<td>161</td>
</tr>
<tr>
<td>transactions</td>
<td>86,88,203</td>
</tr>
<tr>
<td>audit trail</td>
<td>111</td>
</tr>
<tr>
<td>transfers</td>
<td>98</td>
</tr>
<tr>
<td>transport</td>
<td>203</td>
</tr>
<tr>
<td>travel expenses</td>
<td>116</td>
</tr>
</tbody>
</table>
U
unauthorised users .................................. 150
unit testing ........................................... 203
useful reports ........................................ 19,29,38,48,59,68,75,81,90,97,101,105,113,123,135,161,168,175
see also reports
user acceptance testing ............................ 203
user access privileges .............................. 152,156,160
user administration ................................. 151,152
user documentation ............................... 141,144
user exit ............................................. 197,203
user group .......................................... 204
user master records ............................... 153,155,190,204
user parameters ................................. 18
see also super users
user training ........................................ 141,145
users according to complex selection criteria . 161
users locked due to incorrect log-on .......... 161
users with critical authorizations ............. 161

V
validation checks .................................. 86,112,185-86
variant ............................................... 204
vendor account balances ....................... 89
vendor changes (accounting) ................. 75
vendor invoice ................................. see under invoices
vendor master data ............................... 16,86,204
validation of ...................................... 42,45,46,54
vendor master file ................................. 12,13,16,20,23,52,65
authorising changes ............................ 22
vendor master record ............................ 52
vendor number .................................. 24,40,41
vendor master record comparison ........... 25
vendor open items—due dates .............. 39
vendor selection .................................. 11
‘vendor unknown’ .............................. 16
void reason code ................................. 56

W
wage types ........................................... 121,126,128,204
where used lists .................................. 161
workbench organizer ............................ 167,204
workflow ........................................... 12,60,204