IMPORTANT UPDATE

Australian National Audit Office

Human Resource Management Information Systems

Risks and Controls

Better Practice Guide

June 2013

IMPORTANT UPDATE

ISBN 0 642 81335 3 (Print)
ISBN 0 642 81336 1 (On-line)

Executive Director
Corporate Management Branch
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email: webmaster@anao.gov.au

Disclaimer

This Better Practice Guide is not a recommendation or endorsement of the PeopleSoft, SAP or Aurion systems by the ANAO. Australian Government agencies are responsible for deciding whether the PeopleSoft, SAP or Aurion is suitable for their purposes.

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 Better Practice Guide or resulting from their implementation or use of PeopleSoft, SAP or Aurion systems, and to the maximum extent permitted by law, exclude all liability (including negligence) in respect of the Better Practice Guide or its use.

IMPORTANT UPDATE

Foreword

Over the last decade, Australian Government agencies have significantly increased the collection, storage and analysis of human resources data related to their workforce. With functionality now provided by Human Resource Management Information Systems (HRMIS), greater use is being made of automated electronic processes. While there are many efficiencies gained through the use of automated systems, establishing and monitoring internal controls over HR functions are important management considerations—especially if agencies are to provide an assurance over the reliability of their HR information, compliance with applicable laws and regulations, and to effectively and efficiently support business operations.

However, the implementation of HRMIS to support the management of human resources—and the integration of HRMIS with enterprise IT systems—can introduce a range of information management risks. With this in mind, this Guide:

- provides an overview of significant risks and controls that are relevant to key HR functions, with particular focus within each chapter on managing risks through implementation of better practice principles;
- outlines the important role of both system and manual controls in maintaining the integrity and confidentiality of HR information; and
- provides better practice examples for implementing controls for the PeopleSoft, SAP and Aurion HRMIS, which are systems commonly used by Australian Government agencies.

The Guide aims to assist HR system managers and practitioners to:

- implement better practices to improve the effectiveness and efficiency of HR and payroll processes, especially from a security and privacy perspective;
- strengthen system controls and appropriately manage and segregate user access to key system functions; and
- increase awareness of system and manual controls within the PeopleSoft, SAP and Aurion HRMIS used by Australian Government agencies.

The implementation of controls should have due regard to benefits for the agency—equally, reducing controls for cost-saving reasons should be carefully managed as the operating risk profile may be increased. As with all Australian National Audit Office (ANAO) Better Practice Guides, it is important for agencies to individually assess the importance and relevance of practices described in this Guide. This Guide replaces the Guide published in March 2011. The content of the Guide has been refreshed and new sections have been added to reflect the recommended controls—by each of the three HRMIS—to mitigate the risks to key HR functions.

The ANAO expresses its appreciation to contributors to this Guide—Oracle Australia (for PeopleSoft product), SAP Australia and New Zealand, Protiviti, Aurion and the Office of the Australian Information Commissioner.

Ian McPhee
Auditor-General

June 2013

IMPORTANT UPDATE

Contents

IMPORTANT UPDATE

IMPORTANT UPDATE

IMPORTANT UPDATE

1. Introduction

1.1 Purpose of this Guide

The effective organisation and management of HR information is important for the effective functioning of Australian Government agencies[1] and to help achieve their organisational objectives. The use of management information systems, whether in support of financial or human resource functions, assist agencies to gather, store and analyse large quantities of employee data, but agencies also need to ensure the quality and security of this private information. With human resource (HR) and payroll functions closely linked—and changes in one process likely to create issues in another—agencies need to give due consideration on implementing controls to safeguard the privacy, integrity and security of employee information.

"The technology infrastructure is now in place and the key role for the HR IT staff is no longer creating and maintaining systems but making sure the information and workflow meet their...organisational objectives."

Lynne Mealy, President and Chief Executive Officer of the International Association for Human Resource Information Management[2]

This Guide is intended for HR practitioners and system managers in Australian Government agencies, and discusses significant risks and controls relevant to the effective management of key HR functions through the use of Human Resources Management Information Systems (HRMIS). It examines the significant risks and controls that are relevant to four key HR functions conducted in the management of Australian Public Service employees:

- HR and payroll data management;
- workforce management;
- payroll processing and administration; and
- system maintenance and integration.

This Guide replaces the Guide published in March 2011 with:

- refreshed considerations of the significant risks and controls to the four key HR functions, with a focus on risk types associated with financial, fraud, compliance and reporting, and the protection of information; and
- new sections added to reflect the recommended controls for three HRMIS (systems) in use across most Australian Government agencies: PeopleSoft, SAP and Aurion.

1 In this Guide, reference to Australian Government agencies includes government entities subject to *Commonwealth Authorities and Companies (CAC) Act 1997* and the *Financial Management Accountability Act 1997*.

2 As quoted in Kelli W Vito, *Auditing Human Resources*, The Institute of Internal Audit Research Foundation, 2007.

IMPORTANT UPDATE

1.2 Structure of this Guide

The *Human Resource Management Information Systems – Risks and Controls Better Practice Guide* discusses significant risks and controls relevant to key HR functions.

- Part 1 provides an overview of significant risks and controls that are relevant to the key HR functions discussed in the chapter—with details of better practice controls to mitigate the relevant risks; and
- Part 2 examines three HRMIS applications—PeopleSoft, SAP and Aurion, respectively—and provides product specific information concerning better practice and control guidelines when configuring these HRMIS applications.

An overview on each of the chapters in this Guide is set out below.

Part 1 – Risks and Controls to key HR Functions

Chapter 2. HR and payroll data management

Input and maintenance of HR and payroll data poses a significant risk in any HRMIS. It is important that controls are implemented to contribute to the maintenance of HR and payroll data to support accurate and complete employee information and payroll transactions.

This chapter examines general practices for appropriate maintenance of HR and payroll data.

Chapter 3. Workforce management

This chapter examines workforce management activities within HRMIS to strengthen processes associated with the collection and maintenance of employee information, with a particular focus on employee commencements, agency exits and termination of APS employment.

Chapter 4. Payroll processing and administration

This chapter examines risks and controls relevant to time reporting and payroll accounting, with a particular focus on supporting controls relevant to payroll disbursement and posting of payroll expenses to the general ledger that need to be implemented to support accuracy and completeness.

Chapter 5. System maintenance and integration

Various functions and configuration options can be used within HRMIS to enhance the control environment or to increase efficiency within HR management processes. The extent of configuration of system controls varies across organisations. Factors such as entity size, size of the HR team, and whether payroll processing is outsourced contribute to the business requirements to operate and configure controls. The chapter provides an overview on 'additional configurable controls' that may contribute to increasing the efficiency of the HR function and may equally contribute to the accuracy of the HR outputs—and examines the effective management of: system interfaces; system rules; and software updates.

IMPORTANT UPDATE

Part 2 – System–specific Controls

Chapter 6. PeopleSoft Human Capital Management

This chapter is primarily aimed at agencies that use, or may consider using, *PeopleSoft Human Capital Management* HRMIS module (versions 8.9, 9.0 to 9.2). It includes recommended controls to mitigate the risks to key HR functions discussed in Chapters 2 to 5.

Chapter 7. SAP Human Capital Management

This chapter is primarily aimed at agencies that use, or may consider using, *SAP Human Capital Management* HRMIS module. It includes recommended controls to mitigate the risks to key HR functions discussed in Chapters 2 to 5.

Chapter 8. Aurion Human Resources and Payroll Management

This chapter is primarily aimed at agencies that use, or may consider using, *Aurion Human Resources and Payroll Management* HRMIS module. It includes recommended controls to mitigate the risks to key HR functions discussed in Chapters 2 to 5.

Appendices

Appendix 1 to 4 cover:

1. HR information and good privacy practice;
2. Implementing self-service functionality;
3. Glossary of terms discussed in this Guide; and
4. Summary of HR functions with related risks and controls.

1.3 Central themes in this Guide

In any organisation, the HR function is the custodian of a variety of employment data and staff information. In this context, identifying significant risks and implementing effective system controls are essential to safeguard the integrity and security of this information. Key areas that should be considered include:

- managing HR and payroll data;
- legislation and policy compliance;
- risks and controls; and
- segregation of duties.

These key areas are examined below.

Managing HR and payroll data

The input and maintenance of personnel information poses a significant area of risk in any HRMIS. Ensuring that information is updated in the HRMIS in an accurate and timely manner and that updates are authorised is key to the accurate performance of all HR functions.

HR and payroll data are important to effective management of the human resource function. Effective controls over employee information and master data are essential to maintain the integrity and confidentially of employee information. The HR and payroll data management chapter provides further information on significant risks and controls associated with managing master data.

The *Australian Government Protective Security Policy Framework*[3] requires Australian Government agencies to protect information resources, including Information and Communication Technology (ICT) systems, from compromise and misuse. In addition, the Australian Government Information Security Manual (ISM)[4] outlines a combination of physical, personnel, information, IT and communications measures to assist agencies to implement IT security controls that satisfy the minimum standards required to protect information stored or transmitted via electronic means.

This Guide discusses security risks and recommendations for optimising security and access controls for the HR functionality supported by Oracle PeopleSoft, SAP and Aurion applications. Security controls in these applications are inherently complex and require considerable knowledge and skill to implement.[5]

Australian Government agencies are required to comply with the Information Privacy Principles.[6] Good privacy practices are important when dealing with the payroll and human resource processes, given the sensitivity of data being collected and stored.

Legislation and policy compliance

The *Public Service Act 1999* embodies the principles of merit, equity and fairness—and seeks to ensure that employee information is managed with respect during recruitment; at employee commencement and induction; ongoing support in learning and development, performance, health and well-being; and eventual agency exit of termination from the Australian Public Service. Safeguarding the privacy of employee information is therefore important to the Australian Government. Effective controls over managing employee information and processing the payroll reduce the likelihood of errors or the potential for non-compliance with legislation.

Information maintained by agency and entity HR teams is also a key input to internal and external reporting. For example, an agency's Annual Report—incorporating the financial statements—includes a report on executive remuneration and an overview of workforce composition. Further, agencies are required to provide information for other Australian Government reports, such as the State of the Service Report[7] and the annual APS Remuneration Survey.

---

3 The Australian Government Protective Security Policy Framework 2010 is available at the Attorney General's website: http://www.ag.gov.au

4 Department of Defence, *Australian Government Information Security Manual* (ISM), Defence Signals Directorate (DSD), Canberra, 2012.

5 The ANAO has issued other Better Practice Guides, including the *SAP ECC 6.0 Security and Control Better Practice Guide* that outline key measures that can be implemented in SAP environments to improve the security of information.

6 Further information is accessible at: http://www.privacy.gov.au —and refer to Appendix 1.

7 The State of the Service Report provides data and information on changing workforce trends and workforce capability. Section 44 of the *Public Service Act 1999* provides that the Public Service Commissioner must provide a report each year to the Minister for presentation to the Parliament, which includes a report on the state of the Australian Public Service during the year. The State of the Service Report draws on a range of information sources including a survey sent to all APS agencies employing 20 or more staff under the *Public Service Act* and the results of the APS employee survey.

Risks and controls

Controls are generally defined as a systematic measure that is implemented by management to:

- Conduct business in an effective and efficient manner;
- Safeguard assets and resources;
- Deter and detect errors, fraud, and theft; and
- Confirm accuracy and completeness of accounting data.

A commonly asked question is 'What is a relevant control?' While there is no authoritative definition for relevant controls, there are a number of factors that are relevant in determining which controls to implement. For example:

- Relevant controls often support more than one control objective. For instance, user access controls support financial transactions and segregation of duties. In most cases, a combination of relevant controls is an effective way to achieve a particular objective or series of objectives. Placing too much reliance on a single control risks creating a single point of failure.
- Preventative controls are typically more effective than detective controls. For example, preventing a fraud from occurring is far better than simply detecting it after the fact.
- System controls are generally more reliable than manual or process controls and the reliability of these automated controls is dependent upon an entity maintaining an effective control environment. For example, system controls that force periodic changes to user passwords are more reliable than generic policies.

Segregation of duties

Segregation of duties (SOD) is a primary internal control used when undertaking financial operations, which is intended to prevent a single individual from having control over all stages of financial transactions. The objective of segregation of duties is to ensure that different people are involved in the different stages of a transaction—consisting mainly of the initiation, authorisation and approval, recording, and settlement processes. Agencies need to give due consideration against each control and to assess whether an appropriate segregation of duties is in place and enforced.

1.4 How to use this Guide

Each chapter of the Guide identifies key control objectives for the HR function in review—and provides discussion, as relevant to the topic, on those system and manual controls relevant to mitigating or reducing the impact of a risk. Additional controls, often manual in nature, are discussed under the section heading, *Optimising the Control Environment.*

System controls

Most business processes are automated and integrated with other business or corporate systems, resulting in many of the controls at this level being automated as well. System controls include tests that confirm the accuracy of programmed business rules, mathematical calculations, balancing or reconciling control activities, and data validation checks. System controls, being binary in nature, are not subject to intermittent human error. Such controls are generally considered to be more reliable than manual controls, but have an implementation cost in initially configuring the control to support business requirements. The controls that are suggested in this Guide are 'standard' configuration controls that are available through normal licensing terms and conditions for most HRMIS applications.

Additionally, the Guide provides detail on suggested better practice implementation of system controls for the PeopleSoft, SAP and Aurion HRMIS.

IMPORTANT UPDATE

Manual controls

Manual controls (also called process controls) are a management or monitoring practice that may be performed by an agency or entity at its discretion. Often these controls refer to the review or reconciliation of a report to identify irregularities. Such controls are generally considered to be 'detective controls' as they provide information or an output that may be reviewed or analysed in order to detect irregularities. Responses to a number of risks in this Guide recommend the implementation of manual controls as they facilitate validation or 'checks' to confirm that a control activity has been authorised. Such controls often require certain reports to be run from the HRMIS, and the Guide contains information on suggested useful reports which can be generated in each HRMIS.

Key used through the Guide

Risks	Are denoted by 'R' proceeding a reference number
System controls	Are denoted by 'S' proceeding a reference number (range 1 to 39)
Manual controls	Are denoted by 'M' proceding a reference number (range 50 to 65)

Optimising the control framework

The Guide also highlights controls that, if implemented, may improve the efficiency with which an entity performs HR activities or improve the operating effectiveness of existing controls. Such controls often enhance the ongoing activities or processes related to the HR function. With this in mind, implementation of controls should have due regard to the cost benefit involved.

Risk types and classifications used in this Guide

There are numerous methods for classifying and identifying risks. The following is a shorthand approach that has been adopted by the ANAO for the classification of risks in this Guide, while recognising that actual risks may often overlap more than one risk type:

Financial Risk a risk that impacts the financial position of the entity.

Fraud Risk a risk that an intentional deception could be made for personal gain, to damage another individual or the entity.

Compliance and Reporting Risk a risk that the entity could be in breach of Australian legislative or regulatory requirements.

Protection of Information Risk a risk that personal information about individuals could be disclosed without the consent of the individual or that information is not adequately protected.

IMPORTANT UPDATE

Human Resources Management Information Systems – Risk and Controls

Better Practice Guide

Part 1
Risks and Controls to key HR Functions

IMPORTANT UPDATE

IMPORTANT UPDATE

2. HR and payroll data management

Input and maintenance of HR and payroll data poses a significant risk in any HRMIS. It is important that controls are implemented to contribute to the maintenance of HR and payroll data to support accurate and complete employee information and payroll transactions. This chapter examines general practices for appropriate maintenance of HR and payroll data.

Accurate, complete and timely performance of system calculations and reporting is dependent upon the effectiveness of processes associated with management of data in the HRMIS. While employee information may be stored as master data—drawn upon by nearly every activity in the payroll process, including time entry, payroll processing and benefits administration—reference data, such as staff performance management, is subject to periodic change and update. Figure 2.1 shows the importance of master data and its linkages to other HR processes that are discussed in this Guide.

Data in the HRMIS may be categorised as either **master data** or **reference data**, and both are important to the accuracy and completeness of HR functions.

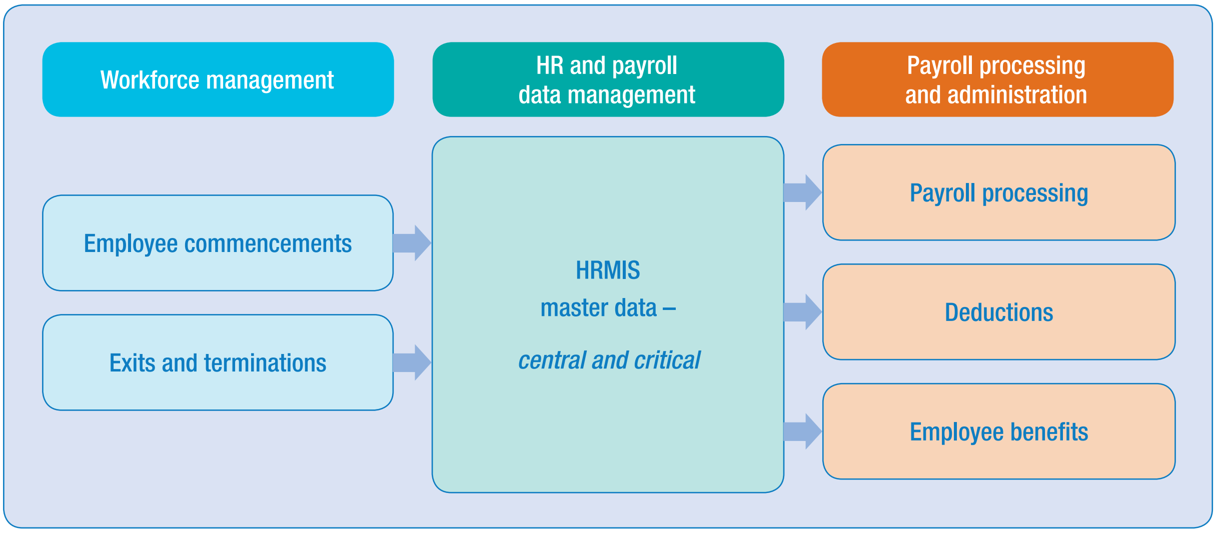
Master data is information that is generally used to support transactional processes and operations, but its use is also central to business analytics and reporting. HR master data includes personal information for example, first name, surname, address, next of kin, salary information and qualifications. Certain types or categories of master data may be considered more sensitive than others (for example, bank details are commonly considered a key data type due to the ability to process fraudulent transactions in an unsecured environment). However, risks and impacts associated with data management are applicable to all types of master data.

Information such as position, conditions of employment, and pay rates are used by several functional groups and may consequently be stored in different data systems across an entity and not be referenced centrally. Effective data management practices assist to prevent and detect such data anomalies.

Reference data is information that is subject to change or update and is important for planning, decision-making or historical references. Reference data, unlike master data, generally does not have explicit definitions to explain the reason for the capture of the data, or for its change and update to the data. The problem to gather, store and make available definitions for individual rows of reference data is not the same as the need to understand the context in the master data. Nonetheless, agencies need to give due consideration to provide quality information through well defined definitions in the reference data.

IMPORTANT UPDATE

Figure 2.1: Master data and linkages to HR processes



2.1 Key control objectives

Control objective	Risks mitigated
HR and payroll data is appropriately maintained to provide accurate and complete employee information and payroll transactions.	**R201:** HR master data is inaccurate. **R202:** HR master data is not secure.

2.2 Legislative and policy compliance considerations

Safeguarding the privacy of employee information is an important consideration—as stated in the *Public Service Act 1990*—that covers the use and disclosure of personal information. And requirements of the Information Privacy Principles for the Australian Government are outlined in Appendix 1. Privacy practices are relevant when dealing with sensitive employee information. HR practitioners should be familiar with requirements relating to collection, storage, retention and disclosure of personal information for current and future employees. Additionally, there are obligations on agencies to comply with the *Australian Government Protective Security Policy Framework* and implement general practices generally to ensure that information is appropriately safeguarded.

IMPORTANT UPDATE

2.3 Managing master data

While adequate processes should be established to securely store hard copy information, it is information stored within system records which is most vulnerable and often subject to unauthorised access. The primary control to protect confidential information is to restrict user ability to perform functions such as to establish, view and amend master data.

Risks and Controls

R201: HR master data is inaccurate	
Risk type	
Consequence	Employee details may be incorrectly entered or maintained, which may result in duplicate payments, errors with superannuation contributions or employee deductions, or unapproved changes to the allocation of roles and delegations.
Better practice	**S01:** *Define key data entry fields.* Key data fields should be defined in the system to confirm that information necessary to the completion of master data is entered. **S02:** *Restricting user access to view, establish and update master data.* Access to view, establish and update master data should be restricted to appropriately authorised users. Users with the ability to view master data should also be appropriately restricted to reduce the likelihood of inappropriate viewing or distribution of data. **S03:** *Validation checks on certain fields warn the user that the information is duplicated in another employee record.* Validation checks should be configured to decrease the likelihood of inaccurate information being entered (for example, tax file number cannot be duplicated in another employee record). **M50:** *Establishment and amendment of master data occurs only when supported by appropriately approved documentation.* All master data established and all amendments processed to master data should be supported by appropriate documentation (approved by an appropriate authority where relevant).

IMPORTANT UPDATE

R202: HR master data is not secure	
Risk type	
Consequence	Unauthorised users may have access to view and maintain sensitive HR and payroll data, which may compromise the confidentiality of personnel records and may also result in the processing of fraudulent payroll payments.
Better practice	**S04:** *Access to HR master data is appropriately configured and managed.* Implementing appropriate user access controls requires: • Identification and implementation of segregation of duty requirements in relation to validating updates/modification/deletion of master data within the HRMIS is complete and appropriately authorised; • Access to the application and to underlying data (such as the database) is assigned based on user profiles and/or roles; and • Employees should be limited in their ability to modify reference data items (salary, leave records and employment date) for their own records. With Web Client applications—like employee self-service (ESS)— the client may allow an employee to be able to modify their own data with the exception of high-risk data fields, including salary, hourly rate, additional pay, job grade. Access controls provide appropriate restrictions to user access to certain data types. Access should be controlled at three levels: • Restrict access to appropriate users (for example, HR personnel but in some situations access may be wider if ESS is implemented); • For each authorised user, restrict access to particular types of master data (for example, only some authorised users will have access to bank details); and • For each user and each type of data, specify whether access is 'view' or 'edit' access. *S02: Restricting user access to view, establish and update master data is also relevant.* **M51:** *Review of system configuration reports.* Generally system configuration change reports are available from the HRMIS and may be reviewed periodically to monitor changes to key controls or configuration settings. Such reports should be run periodically. Consideration should be given to ensuring that appropriate 'audit' tables and associated logs are also configured. Failure to configure such tables may mean that important information is not available for inclusion in monitoring reports.

Optimising the control framework

Control item	Description
Clean desk policy and appropriate filing of hard copy employee records	Within HR and payroll teams, care must be taken to appropriately store hard copy documents containing sensitive employee master data. A 'clean desk' policy and policies around shredding and retention of documentation should be considered, and the appropriate use of document security classification.

IMPORTANT UPDATE

3. Workforce management

This chapter examines the workforce management activities within HRMIS to strengthen processes associated with the collection and maintenance of employee information, with a particular focus on employee commencements, agency exits and termination of APS employment.

Workforce management is a key strategic consideration for government agencies, covering a range of activities and actions, such as: recruitment of employees, learning and development, succession planning, rewards and recognition, absence management and performance management.

3.1 Key control objectives

Control objective	Risks mitigated
Appropriate and accurate employee information is collected and maintained.	**R301:** Non-existent or duplicate employee is added to the payroll. **R302:** Termination payments and balances are inaccurately calculated. **R303:** Employee is not deactivated when employment is terminated.

Part 1: Risks and controls to key HR functions

3.2 Legislative and policy compliance considerations

Activities undertaken within the workforce management process are subject to various legislative and policy compliance requirements. The key legislation and policy matters relating to Workforce Management include:

Legislation and policy framework	Purpose
Public Service Act 1999	Governs the establishment and operation of, and employment in, the Australian Public Service. Part 4 of the Act addresses methods of setting employment terms and conditions, employee transfers between agencies and termination of employment requirements.
Public Service Regulations 1999	Parts 3 and 8 of the Regulations deal with issues in relation to APS employees. These include matters such as: the date of effect of promotions and the engagement of an employee for a specified term (Part 3); and terms and conditions of employment of APS employees after machinery of government changes (Part 8).
Public Service Commissioner's Directions 1999	The Commissioner's Directions regulate matters including the engagement and promotion of APS employees (Chapter 4) and a wide variety of matters in relation to the employment of SES employees (Chapter 6).
Public Service Classification Rules 2000	The Classification Rules detail the permitted classifications of APS employees and requirements around moving employees from training classifications to ordinary classifications.
Part 11 of the Financial Management and Accountability Regulations 1997	The *Financial Management and Accountability Regulations 1997* are made under the *Financial Management and Accountability Act 1997*. Their purpose is to ensure accountability and consistency across Commonwealth Government entities. Part 11 relates to the method of accounting for the transfer of leave entitlements for employees moving between agencies.

IMPORTANT UPDATE

Legislation and policy framework	Purpose
Privacy Act 1988 (Cth)	Regulates collection, use, and storage by federal government entities of personal data. Commonwealth agencies are required to comply with the Information Privacy Principles which are set out in section 14 of the Act.
Work Health and Safety Act 2011	The Act sets out a framework to secure the health and safety of workers and workplaces by: protecting workers and other persons against harm to their health, safety and welfare through the elimination or minimisation of risks arising from work; providing for fair and effective workplace representation; promoting improvements in work health and safety practices; and providing a framework for continuous improvement and progressively higher standards of work health and safety.
Safety, Rehabilitation and Compensation Act 1988	An Act relating to the rehabilitation of employees of the Commonwealth and certain corporations and to workers' compensation for those employees and certain other persons, and for related purposes.
Fair Work Act 2009	Regulates employment and industrial relations in Australia in relation to all national system employers (including the Commonwealth of Australia) and their employees. The Act sets out certain minimum terms and conditions of employment (the National Employment Standards) in relation to matters such as leave entitlements, notice of termination, and redundancy pay. These are contained in Part 2-2 of the Act.
Other legislation relevant to recruitment and selection	• *Administrative Decisions (Judicial Review) Act 1977* • *Age Discrimination Act 2004* • *Australian Human Rights Commission Act 1986* • *Disability Discrimination Act 1992* • *Fair Work Act 2009* • *Freedom of Information Act 1982* • *Privacy Act 1988* • *Racial Discrimination Act 1975* • *Sex Discrimination Act 1984* • *Spent Convictions Provisions in Part VIIC of the Crimes Act 1914*

IMPORTANT UPDATE

3.3 Employee commencements

The employee commencement process encompasses identification of the requirement to fill a vacant role or create a new role, approval to seek and appoint an individual, selection of the individual and the administration associated with the recruitment.

Upon acceptance of the offer, the new employee is required to provide personal information to enable set-up of an employee record on the HR and payroll systems (refer HR and payroll data management). A considerable amount of information relating to the successful applicant is required—ranging from transfers and promotions, to planned working time and salary and leave entitlements.

Given the sensitive content of conditions of employment it is important to consider the Australian Government Information Privacy Principles (see Appendix 1). Principle 4 requires a record-keeper (agency or entity) to protect the record (employment contract) by such security safeguards as it is reasonable in the circumstances to take, against loss, unauthorised access, use, modification or disclosure and any other misuse.

Position management

Position management is critical to ensure employees are allocated to a particular role or position. Attributes associated with a position description include: the pay rate and benefits.

Employees may occupy more than one position in the following ways:

- Permanent transfer: making a permanent move;
- Temporary transfer: making a short-term move from one position to another; or
- Higher duties: occupying more than one position for a defined purpose and for a short period of time.

There are several approaches that may be used to reflect this in the HRMIS. In the first two instances, it is likely that the employee's record will be modified to reflect the change in position. In the third instance, where the employee works within his or her own position, and a higher position, the time spent in the higher position may be controlled through the time reporting process and receive additional benefits via the payroll process. The functionality to manage employee positions within the organisational chart is discussed further in Chapter 5 *System Maintenance and Integration.*

Transfers and promotions

A transfer in the context of the HR process may mean one of the following:

- Intra-agency transfer: an APS employee moving to a different position within the same agency or entity; or
- Inter-agency: An APS employee moving from one agency or entity to another.

A key objective in managing employee transfers, either inter-agency or intra-agency, is to transfer complete and accurate records relating to that employee, particularly accrued benefits.

Risks and controls associated with inter-agency transfers are similar to risks associated with the employee commencement and exit process—and is addressed in *Agency exits and termination of APS employment.*

An additional risk for inter-agency transfers involves the transfer of leave entitlements and other benefits. The risks generally with intra-agency transfers relate to controls associated with the management of positions in the HRMIS—and is addressed in Chapter 5 *System Maintenance and Integration*.

IMPORTANT UPDATE

Risks and Controls

R301: Non-existent or duplicate employee is added to the payroll	
Risk type	
Consequence	‘Ghost’ or duplicate employees on the payroll lead to overpayment or processing of fraudulent payments.
Better practice	**S05:** *Access to add an employee should be restricted to appropriate individuals and segregated from payroll maintenance.* Access to modify employee information should be restricted to decrease the likelihood of inappropriate or unapproved changes to employee information which may impact upon the accuracy and completeness of information maintained in the HRMIS. Additionally, restricting access in accordance with privacy principles reduces the risk of inappropriate disclosure of employee information. *Also refer to **S03**: Validation checks on key fields warn the user that the information is duplicated in another employee record.*
	M52: *When adding a new employee, a listing of current employees should be reviewed to reduce the risk of duplicating the employee record.* A system report of all current employees should be generated prior to adding a new employee, and checked to confirm the employee does not already exist in the system. A system report of all new employee additions should be generated monthly and an individual who is independent from the employee set-up process should check each addition against supporting paperwork (for example, approval to engage, employee information including bank account) to validate the set-up was authorised and has been completed accurately.

IMPORTANT UPDATE

Optimising the control framework

Generally, determining employee conditions of employment is performed outside of the HRMIS. It is important that the organisation hierarchy and payroll calculation rules are established and maintained to provide consistency with conditions of employment. Further detail on configuring key system controls or implementing supporting manual controls is provided in Chapter 5 *System Maintenance and Integration.*

The following items should be considered when managing the employee commencement process:

Control item	Description
Development of standardised reference and background check procedures	A security clearance and reference checking policy should be developed and documented prior to employee commencement. Sign-off certifying compliance with this standard should be obtained for each selected candidate prior to progressing to appointment stage. Documentation supporting the background/reference checking and security clearance should be retained.
Information collected during the application process is handled in accordance with Privacy legislation	Training on Information Privacy Principles and obligations placed upon those responsible for handling and retention of personal information should be provided to all employees involved in the employee recruitment process.
Managing transfer requirements	Part 11 of the *Financial Management and Accountability Regulations 1997* stipulates arrangements for transfer of employee leave entitlements when employees move between agencies.
A standard employee appointment form is used to document new employee details and is appropriately authorised before the new hire is entered into the system.	A new employee commencement template form should be developed and utilised to capture key information to be keyed into the system, including employee personal details and HR information such as salary and position. This form should be signed off prior to entry of information into the system.

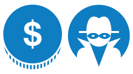
IMPORTANT UPDATE

3.4 Agency exits and termination of APS employment

In the event an employee is terminating their employment from the Australian Public Service—as opposed to a transfer[8] to another agency—the employee exit process is initiated when either the employer or employee provides notice of termination. At the employee's date of termination, a termination payment is calculated. The employee returns all property owned by the employer, and the employee's logical and physical access is removed. A termination payment is the final payment made to an employee which incorporates payout of all entitlements. The payment will include salary/wages for all days worked and the payout of leave entitlements in line with policy or legal requirements.

Amounts may be deducted from termination payments based on policy or agreed Conditions of Employment. These could include, for example, relocation or study costs paid to the employee may be recovered if the employee is terminated within a defined period. In instances of involuntary termination or retirement, a termination package inclusive of additional entitlements may need to be calculated. Termination payments are made as a one-off payment on the date of termination, or included in the next pay run.

Risk and controls

R302: Termination payments and balances are inaccurately calculated	
Risk type	
Consequence	Termination payment is incorrect, resulting in incorrect salary and leave entitlements being paid or reported
Better practice	**S06:** *Application will warn user if termination date in the past is entered.* The system should be configured such that if a termination date in the past is entered, a warning message is generated to reduce the occurrence of backdating of terminations and to accurately process termination payments and calculations. **S07:** *Workflow operates to require independent approval verification of termination date entered.* Automated workflow approvals utilising organisation hierarchy positions delegations of authority should be utilised to approve terminations. The approver should verify the termination date of the employee prior to approving. **S08:** *Application automatically calculates payments based on master data, termination date entered, and leave entitlements.* Use of system functionality to calculate and report entitlements and balances is more accurate. The effectiveness of this control requires accurate data entry and maintenance of employee information and master data. **M53:** *An independent authority checks the termination date per notification documentation to the date entered in the system.* On a monthly basis, a report of all terminations is generated and an individual who does not have access to terminate employees checks that all termination dates were accurately entered, with reference to termination documentation (for example, resignation letter).

8 Employee transfers across agencies are subject to section 25 of the *Australian Public Service Act*—and are not considered employee terminations from the Australian Public Service but departmental transfers.

IMPORTANT UPDATE

R303: Employee is not inactivated when employment is terminated	
Risk type	
Consequence	Employee record is not flagged as terminated which may result in subsequent payment to the employee. For agencies using 'single sign on' (which enables access to all applications without requiring separate passwords, by using credentials at the network sign-on level), failure to inactivate terminated employees may also fail to inactivate network access.
Better practice	**S09:** *Application automatically changes status of employee to 'terminated' as at termination date entered.* Systems are configured to automatically change the status of employees to 'terminated' as at the entered termination date. This is typically enabled through automated batch processing. **S10:** *Application automatically disables terminated employee's access to systems based on termination date entered.* This control is possible where position-based security is utilised. Appropriate use of the termination date is important where single-sign access is granted based on a commencement or termination date. **S11:** *Application does not allow payment to be disbursed to employees with 'terminated' status.* Operation of this control typically does not require specific configuration within the system, as it is deemed 'standard' functionality. It may be possible in some circumstances to process ad-hoc payments to terminated employees using some applications **M54:** *Department/Cost Centre managers are periodically provided with a listing of employees for which they are responsible. This listing is checked to determine whether it contains any employees no longer working within the department.* System generated listings of current employees per department/area/cost centre should be provided to relevant managers to verify current employees. This check assists in detecting employees who have transferred or been terminated and information regarding the transfer or termination has not been recorded in the system.

Optimising the control framework

The following items should be considered to improve management of employee information relevant to employee departures:

Control item	Description
'Employee Exit' checklist	An employee exit checklist assists HR in completing all steps to mitigate risks associated with employee termination. The checklist should include the requirement to return all entity property from the terminated employee and remove physical and system access.
Reconciliation of terminations	A listing of terminations is maintained external to the system by the HR section as notifications are received. This listing is reconciled to a listing of all terminated employees within the system each month. Performing a check of an external record of terminations against a system generated listing on a monthly basis assists in ensuring all terminations have been recorded in the system in the correct period.

IMPORTANT UPDATE

4. Payroll processing and administration

This chapter examines risks and controls relevant to time reporting and payroll accounting, with a particular focus on supporting controls relevant to payroll disbursement and posting of payroll expenses to the general ledger that need to be implemented to support accuracy and completeness.

Payroll processing and administration is highly dependent on two related functions and activities:

- **Accuracy**: the payroll calculation will only be accurate if using complete and accurate master data (see HR and payroll data management and Workforce management chapters for discussion on risks and controls related to obtaining and managing HR data).
- **Completeness**: the payroll processing will only be accurate if employee time and leave requests have been correctly captured and all deductions have been properly processed.

4.1 Key control objectives

Control objective	Risks mitigated
Evidence of employee service and time is accurately recorded in the appropriate period.	**R401:** Inaccurate or incomplete entry of employee time data. **R402:** Unapproved leave or leave is taken outside of entitlements. **R403:** Established employee shifts are updated inaccurately. **R404:** Time recorded in prior periods is amended inaccurately or without appropriate authority.
Accurate process employee payroll for each pay period.	**R405:** Payroll calculation is inaccurate or incomplete.
Gross pay and deductions are accurately calculated and only applicable deductions are processed.	**R406:** Statutory obligations for payment of taxation are breached. **R407:** Breach of legislative requirements relating to superannuation. **R408:** Salary sacrifice arrangements are not appropriately managed.
Additional payments to employees that relate to performance payments or other regards are accurately calculated and approved prior to disbursement.	**R409:** Methodology for performance payments is not established. **R410:** Employee benefits are not managed or administered in accordance with Workplace Agreements/employee contracts.

IMPORTANT UPDATE

4.2 Legislative and policy compliance considerations

Activities undertaken by the payroll processing and administration process are subject to various legislative and compliance requirements. The key legislative and policy matters relating to payroll processing and administration include:

Legislation and policy framework	Purpose
Long Service Leave (Commonwealth Employees) Act 1976	Sets out the conditions of eligibility, accrual and payment of long service leave for Commonwealth employees.
Maternity Leave (Commonwealth Employees) Act 1973	Sets out the paid and unpaid maternity leave arrangements for Commonwealth employees. Employers often provide supplementary maternity leave benefits in collective/enterprise agreements.
Safety Rehabilitation and Compensation Act 1988	Sets out the Commonwealth's liability to pay compensation to employees who are injured in the course of their employment and the procedures for calculating and making the payments.
Governance of Australian Government Superannuation Schemes Act 2011	The Act established governance arrangements for the Commonwealth superannuation schemes that are effective and more consistent with the broader superannuation industry. A single trustee is responsible for managing the main Commonwealth civilian and military superannuation schemes, and are the: • Commonwealth Superannuation Scheme (CSS) • Public Sector Superannuation Scheme (PSS) • Public Sector Superannuation Accumulation Plan (PSSAP) • Military Superannuation and Benefits Scheme (MSB) • Defence Force Retirement and Death Benefits Scheme (DFRDB) • Defence Forces Retirement Benefits Scheme (DFRB) • Defence Force (Superannuation) (Productivity Benefit) Scheme (DFSPB).

4.3 Time reporting

Most HRMIS embed standard hours of work for each agency, and then capture employee times against overtime, absences, shifts, and agreed part-time arrangements—important in the support of both HR and payroll functions. Where an employee is required to perform higher duties in addition to duties at their designated level, hours worked may also be recorded against each position.

There are also a number of other ways in which 'working time' may be utilised, including various types of absences, breaks, time travelling for business purposes, or time outside the entity's standard working hours. These hours need to be captured and accounted for in accordance with entity policy or procedures. Time is typically recorded in timesheets. This is also often the case for salaried employees, and timesheets allow tracking of time allocations by activity or project.

A further consideration in the accurate processing of the payroll is management of the work roster. In general terms, a work roster is a listing of employees and their assigned work hours. For example, the dates or days of the week that an employee would be expected to be present to undertake work or is expected to be on leave of any type. Further information within a work roster may include detail at an hourly level, and/or projects or tasks to which each employee is assigned during working hours.

IMPORTANT UPDATE

Risks and controls

R401: Inaccurate or incomplete entry of employee time data	
Risk type	
Consequence	Time data entered does not accurately reflect time worked or does not include leave taken. Employee receives payment for hours or leave to which they are not entitled.
Better practice	**S12:** *Workflow approval of employee time.* Where workflow functionality is used, such as in self-service, the workflow should be configured so that submitted employee time is automatically routed through the workflow approval hierarchy for review by the employee's immediate supervisor or functional manager. The workflow should also be used to send rejected time allocations or leave requests to the employee via the system with the reason recorded. **S13:** *System validation of data entered.* Validation checks should be configured to decrease the likelihood of inaccurate time being entered (for example, minimum/maximum number of working hours, checks against established time codes). The system may also be configured to provide default timesheets to employees with standard responsibilities and working hours. **S14:** *Timesheets are locked for editing after submission.* After submission, the system should restrict employees from being able to edit time submitted. In order to alter time, a prior period adjustment must be processed. **S15:** *Automated notifications.* Automated notifications remind users to enter their time report, and continue to alert users when the time reporting deadline is reached and passed. **M55:** *Review 'Missing Time' report.* Immediately after the time reporting deadline, the payroll department should generate a report outlining missing time and follow up directly with employees and the employees' functional managers.

IMPORTANT UPDATE

R402: Unapproved leave or leave is taken outside of entitlements	
Risk type	
Consequence	Employee takes leave which is either not recorded on timesheets, or when recorded results in the employee having a negative leave balance.
Better practice	**S16:** *Automated checks on leave applications to confirm sufficient entitlement.* Use of system functionality to capture leave requests will enable comparison reporting to be generated and show any discrepancies between leave recorded in timesheets and leave requested. **S17:** *Workflow approval of leave requests.* System functionality to process leave requests (for example, Employee Self Service) should be utilised to enable automated checks to be performed against employee entitlements and leave balances. Requested leave should route through the workflow approval hierarchy for approval prior to the request being approved. The application should be configured to raise a 'warning flag' if the requested leave will result in negative entitlement balances. **M56:** *Periodic review over recording of leave.* A two-way check should be performed by the payroll team on a monthly basis to confirm that: • Leave taken by employees in reflected in timesheets; and • Leave recorded was appropriately approved. Any discrepancies should be followed up with the employee and the employee's immediate supervisor.

R403: Established employee shifts are updated inaccurately	
Risk type	
Consequence	Inaccurate employee shifts reporting may lead to inaccurate payroll processing and may impact leave accrual calculations.
Better practice	**S18:** *Restrict user access to amend employee shifts.* Access to update employee shifts should be restricted to appropriate personnel and employees should not have access to update their own shift details. **M57:** *Approval of updates to employee shifts.* Employee shifts should only be updated in the system following approval by an appropriate authority.

IMPORTANT UPDATE

R404: Time recorded in prior periods is amended inaccurately or without appropriate authority	
Risk type	
Consequence	Inaccurate or unauthorised adjustments lead to inaccurate leave balances or time reporting.
Better practice	**S19:** *Restrict user access to process prior period adjustment.* Access to process prior period adjustments should be restricted. This may require a procedure to be put in place whereby a manual request (appropriately approved) is submitted. **S20:** *Workflow approval of prior period adjustments.* Amendments to time recorded in prior periods should be processed through the workflow approval hierarchy. **S21:** *Limit prior period adjustments.* The system should limit the prior period for which adjustments can be processed (e.g. four weeks, or a small number of immediate past periods). **M58:** *Approval of prior period adjustments prior to processing.* When a prior period adjustment is required, the details are documented on a standard form requiring approval from an appropriate authority prior to processing. The adjustment is then processed in the system by a member of the payroll team. **M59:** *Review prior period adjustments.* On a monthly basis, a report should be generated that lists all prior period adjustments processed. This report should be reviewed to determine the appropriateness of adjustments processed.

Optimising the control framework

The following items are additional activities that assist in the completeness and accuracy of employee time and leave information:

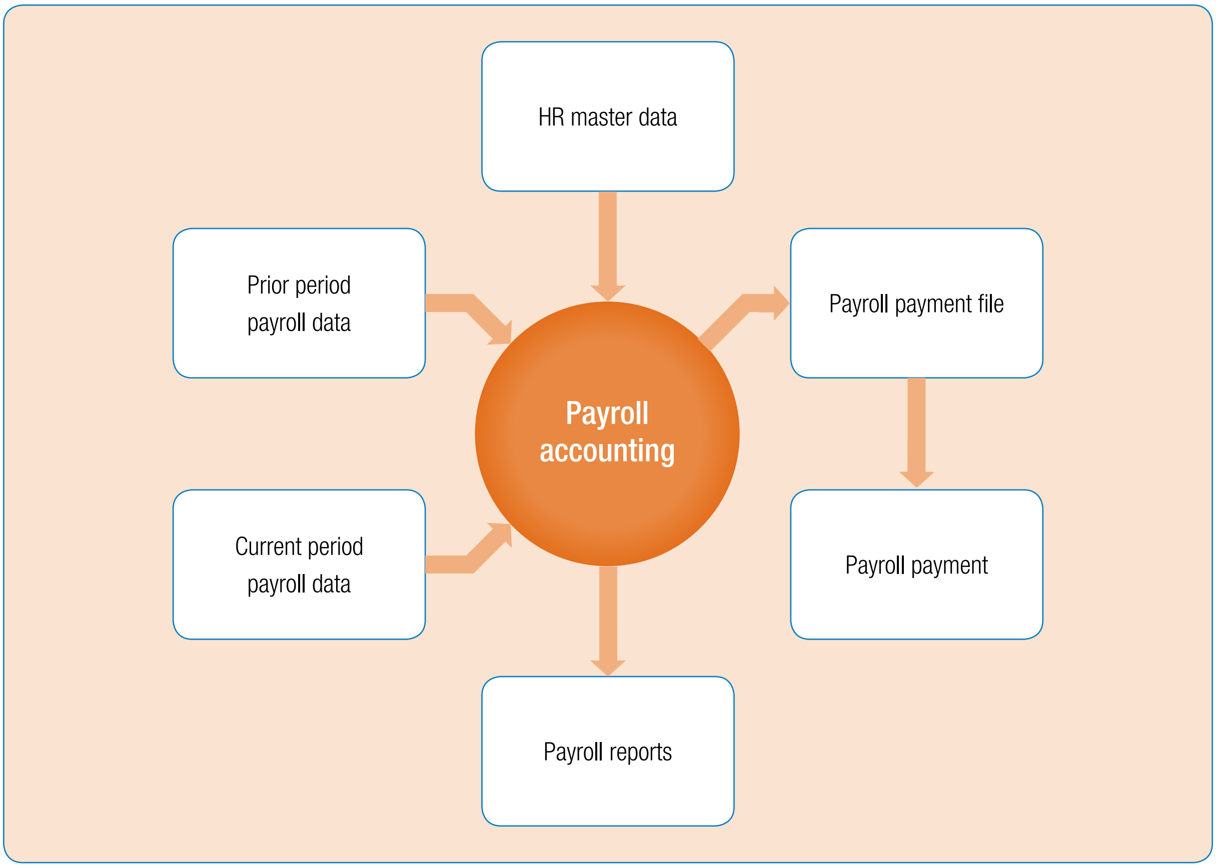
Control item	Description
Use standard leave forms	Where electronic Employee Self-Service functionality is not implemented, a standard leave form should be used to record employees' requests for leave. All leave requests should be submitted by the employee and approved by the employee's immediate supervisor. In considering the leave request, the approving officer should have regard to the employee's entitlements and any approval resulting in negative leave balances should note the reason (or be in line with entity policy allowing negative leave balances).
Authorisation of amended timesheets	Amendments to submitted time should be initialled by the person making the amendment and appropriately approved before being updated in the system. If amended by someone other than the employee, the employee should be notified of the amendment.

IMPORTANT UPDATE

4.4 Payroll accounting

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

Figure 4.1: Overview of the payroll processing and administration function



Pay run processing

The payroll payment function is the process of approving the payroll calculation for payment to employees and processing the payment to employees' financial institutions and other recipients. Payment is typically made using an electronic banking application installed on a secure terminal. The payroll information in the payroll system may automatically interface to this software, or may need to be manually downloaded from the payroll system and uploaded to the banking software.

The pay cycle process includes calculating and disbursing the payroll payment. The payroll calculation function involves performing the periodic calculation of employee costs. This calculation is typically automated, drawing upon employee master data and electronically captured time reporting.

While not configurable in the HRMIS, the following should be considered key controls:

- The file used to transfer payroll information from the HRMIS to the banking package being stored securely during transmission, and in an un-editable format; and
- Dual authorisation of disbursement within the banking package.

Part 1: Risks and controls to key HR functions

System controls are essential to protect against errors and fraudulent transactions. There are a number of manual controls that may provide increased assurance over the pay run process. In particular, reconciliation of amounts disbursed via the banking package (EFT transfers) and the final approved pay run report (payroll calculations and transfer of expenses to the General Ledger) is important to validate that the payroll disbursement is accurate. Similarly, the bank reconciliation process is also an important detective control to confirm payments were processed completely and accurately.

Taxation and other statutory deductions

A payroll deduction is an amount withheld by the entity from an employee's earnings. Typical deductions are personal income tax and superannuation contributions.

Employers are obligated to withhold Pay As You Go (PAYG) amounts from salary or wage payments made to employees. This involves the employer:

- Registering with the Australian Taxation Office (ATO) for PAYG withholding;
- Establishing the status of each of their employees;
- Determining the amount to be withheld;
- Withholding this amount and remitting it to the ATO;
- Providing each employee with a payment summary showing the total payments the employer made and the amount the employer withheld for each employee during the financial year; and
- Lodging an annual report summarising the amounts paid to the ATO.

Employers may also be liable for Fringe Benefits Tax if benefits are provided to staff because they are employees of the entity. Benefits include rights, privileges or services, such as allowing an employee to use a work car for private purposes. Employers may also be required to withhold garnishments as legally required, for example by court orders.

Superannuation

An employer is required by legislation to pay superannuation contributions into a complying superannuation fund by a specified cut-off date for all eligible employees. The amount of superannuation payable is determined by the applicable legislation.[9]

Accumulated contribution schemes

Since 1 July 2006, Australian Government employers have been required to offer choice of superannuation fund to members of the Public Sector Superannuation Accumulation Plan (PSSap) and new employees and new statutory office holders (eligible choice employees) in accordance with the *Superannuation Guarantee (Administration) Act 1992* (SG Act).[10]

In addition to the mandatory employer contribution, an employee may elect to make employee contributions to the fund. Employees can generally make personal (after-tax) contributions through a payroll deduction or by a payment directly to the fund. From 1 July 2009, where the employer allows it, employees can also make pre-tax contributions through a salary packaging arrangement. These pre-tax contributions are considered employer contributions.

The amount withheld during the payroll calculation is remitted to the relevant fund(s) as a lump sum via the normal electronic banking process. Reporting provided to the funds specifies amounts attributable to each employee. The superannuation fund(s) take responsibility for crediting employee superannuation accounts appropriately and paying applicable taxes.

9 See list of relevant superannuation legislation discussed earlier in *Legislative and policy compliance considerations*.

10 Department of Finance and Deregulation, Choice of Superannuation Funds for New Australian Government Employees [Internet], Department of Finance and Deregulations, Australia, 2011, available from http://www.finance.gov.au/superannuation/arrangements-for-australian-government-employees/choices-of-fund-for-new-aps-employees.html [accessed 02 April 2013].

IMPORTANT UPDATE

Defined benefit schemes

Australian Government employees who commenced employment prior to 1 July 1990 or 1 July 2005 may be members, respectively, of the Commonwealth Superannuation Scheme (CSS), Public Sector Superannuation (PSS) scheme, while military personnel may be members of the Military Superannuation and Benefits scheme (MilitarySuper) and the Defence Force Retirement and Death Benefits (DFRDB) scheme. These are defined benefit superannuation schemes—and their administration differs to that of accumulated contribution schemes in that the amount and timing of employer contributions to funds is determined annually by the fund after consultation with actuaries, with the contribution percentage for each fund advised to agencies by the Department of Finance and Deregulation.

An effective control framework introduces processes and controls that support compliance with legislative requirements, for example, that sufficient superannuation is paid and remitted to the selected fund in a timely manner, and document retention systems are in place.

Salary sacrifice

A salary sacrifice arrangement is also commonly referred to as salary packaging or total remuneration packaging. It is an arrangement between an employer and an employee whereby the employee agrees to forgo part of future entitlement to salary or wages in return for the employer providing benefits of a similar value. Typical benefits associated with salary sacrifice arrangement involve superannuation contributions or leasing a motorcar.

Performance bonuses

Performance bonuses are cash payments typically made on an annual basis and disbursed in conjunction with the standard payroll processing. The amount each employee receives may be formula driven and linked to performance against a set of performance criteria. Alternatively, the amount attributed to each employee may be discretionary and determined by the employee's manager. An accrual should be maintained for the performance amount, whether calculated via formula or discretionary. Adjustment of the accrual within the General Ledger is likely to be performed via a manual journal rather than interface from the payroll or HR module.

Where performance bonuses are based on a percentage of employee base salary or can be calculated using data established in the system, the automated accrual and payment calculation should be utilised for accrual and calculation purposes.

Other benefits

Other benefits may be available to employees in addition to their salary. Whether an employee is eligible for a benefit will often depend on that employee's position and/or the terms and conditions of their employment agreement. Additional benefits offered may include an allowance towards child care and car parking fees.

Most additional benefits require the employee to elect whether they wish to take up the opportunity to receive that benefit, and the employee election is recorded in the employee's master data (see HR and payroll data management).

Benefits will typically be administered as part of an overall salary package, or as a deduction to the employee's earnings. Controls over the deduction master data are a prerequisite for administration of benefit arrangements.

Generally, large HRMIS applications manage administration of benefits by identifying attributes and parameters of the 'benefit plan' in the system, and identifying which employees are eligible for the benefit and have opted to receive the benefit.

Payroll exception reporting is particularly useful for verification of bonus payment where normal payroll payments are relatively stable. The variation between the pay period in which bonus payments are made and the prior pay period should align to the approved bonus amount.

IMPORTANT UPDATE

Risks and controls

R405: Payroll calculation is inaccurate or incomplete	
Risk type	
Consequence	Draft payroll proposals are not reviewed for reasonableness prior to finalisation of the payroll, resulting in failure to detect significant anomalies or errors.
Better practice	**S22:** *Restrict changes and user access to modify payroll calculation rules.* Personnel calculation rules are used to calculate gross and net pay for employees and should be protected from being overridden or modified without appropriate authorisation. **M60:** *Review payroll control reports and variance reports.* Useful reports to review prior to finalisation of the payroll include: • Payroll Exception Reports are effective where there is little variation between pay periods. Approved documentation such as leave forms, new engagements, terminations, change in pay rate, and change in deductions should be available to justify the period variation; • Payroll Budget to Variance Reports are effective in identifying significant differences; and • Employee Changes Reports highlight new employees, terminated employees and transfers to ensure only current and valid employees are included in the pay run. Once the reviewer is satisfied with the payroll calculation, a final payroll report should be produced and a copy filed.

R406: Statutory obligations for payment of taxation are breached	
Risk type	
Consequence	ATO requirements including PAYG and FBT payment requirements, are breached through failure to retain adequate records or report on and remit tax by specified deadlines, potentially resulting in penalties or reputational consequences.
Better practice	**S23:** *Restricted access to establish and amend taxation reference tables.* The ability to upload and amend tax tables within the HRMIS should be restricted and changes to reference data should be approved prior to the change being implemented. **M61:** *Review and approval of Fringe Benefits Tax return by appropriate authority.* The amount of FBT payable is self-assessed by the entity. Prior to lodgement of the annual FBT return, detailed review should be undertaken by an appropriate person to determine whether: • Confirmation that a fringe benefit which has been provided is accurate; and • Where a fringe benefit has been provided, the applicable rates and thresholds have been accurately applied in the calculation outlined within the return.

IMPORTANT UPDATE

R407: Breach of legislative requirements relating to superannuation	
Risk type	
Consequence	Insufficient superannuation is paid, or payment is not made prior to the quarterly cut-off date. ATO guidance is contravened due to failure to retain adequate documentation in support of super contributions.
Better practice	**S24:** *Configure automated calculation of superannuation payable.* Flagging employees as eligible or ineligible for super contributions and setting the percentage of super payable should enable the super amount payable per period to be automatically calculated by referencing the payroll calculations (for salaries and wages paid) and relevant master data, such as salary sacrifice amounts and additional employee contributions.

R408: Salary sacrifice arrangements are not appropriately managed	
Risk type	
Consequence	Salary sacrifice arrangements are not clearly documented and the components are not captured in the HRMIS, leading to inaccurate taxation calculations, payments, and disbursements. Non-allowable items are included as part of a salary sacrifice arrangement. This may lead to inaccurate fringe benefits and PAYG tax calculations.
Better practice	**S25:** *Salary sacrifice details are appropriately established in the HRMIS.* The ability to establish and amend salary sacrifice details in the HRMIS should be restricted to appropriate roles within the entity, having regard to enforcing effective segregation of duty controls. **M62:** *Review and monitor changes to key salary sacrifice information.* Set-up of the salary package elements and rules should be independently reviewed to ensure the following: • Configuration accurately reflects the documented salary sacrifice agreement; • The salary/wage component has been accurately captured to enable accurate PAYG withholding; • Sacrifices which constitute fringe benefits have been accurately classified and captured to enable accurate Fringe Benefits Tax self-assessment; • Sacrificed superannuation is set up as an employer contribution (to be subject to taxes associated with this type of contribution) effective 1 July 2009; and • Salary package elements outside the policy framework are not included as part of the arrangement.

IMPORTANT UPDATE

Taxation calculations may be largely automated when correctly configured. The calculation is highly dependent on accurate upload of the most recent taxation tables from the ATO.[11] Automated updates should be configured to assist in ensuring tax information remains current (see System maintenance and integration for discussion on system updates).

Records for employees who are members of defined benefit superannuation schemes should be updated annually to adjust the percentage payable to the defined benefit fund.[12] Employees who are members of accumulated contribution schemes will be flagged as such, and the defined percentage[13] will apply to those employees' records. By recording the relevant percentage against each employee record, calculation of the amount to be remitted to the superannuation funds may be automated through the HRMIS.

Generally, there are no standard 'audit' or 'control' reports associated with payroll deductions. The majority of detail around deductions is contained in normal pay run reporting.

R409: Methodology for performance payment is not established	
Risk type	
Consequence	Unauthorised or inaccurate bonus payments may be disbursed to employees. Bonuses may not be adequately accounted for throughout the period.
Better practice	**S26:** *Utilise system functionality to accrue for and calculate bonus payments.* Where bonus payments are based on a percentage of employee base salary or can be calculated using data established in the system, the automated accrual and payment calculation should be utilised to reduce the risk of inaccurate accrual and calculation. Where automatically calculated, the system output should be independently reviewed by an authorised HR representative for accuracy.

R410: Employee benefits are not managed or administered in accordance with employee agreements	
Risk type	
Consequence	Employees may receive benefits to which they are not entitled, potentially resulting in financial loss to the entity. Entity may breach terms of enterprise agreements through poor management of employee benefits process.
Better practice	**S27:** *Correctly establish and manage employee benefits.* Eligibility for employee benefits should be established by pay structure/employee role/employee type. When adding a participant, the system should be configured automatically to reference the position (if eligibility is based on level in the organisation) and should prevent participation of ineligible employees or employee classifications. If eligibility is based on information contained in master data (for example, years of service), master data should be automatically referenced to block participation of ineligible employees. **S28:** *Restricted access to establish benefit plans.* Access to establish benefit plans, enrol employees, create employee specific information associated with the plan and amend plan or employee information should be restricted to appropriately authorised personnel.

11 Refer to www.ato.gov.au for tax withholding tables.
12 The amount to be contributed for each employee is set out in an annual letter from the Department of Finance and Deregulation.
13 The percentage payable at the time of publishing is 15.4% under the legal authority of the *Superannuation Act 2005*.

IMPORTANT UPDATE

Optimising the control environment

The majority of payroll payments are processed through electronic funds transfer. Inadequate controls operating over EFT payments may result in incorrect payments and financial loss for the entity. Better practice procedures which should be implemented to ensure that disbursement of payroll files and information is authorised and accurately processed are highlighted below:

Control item	Description
Develop policy around information retention	A policy should be developed and communicated to relevant HR and payroll team members that specifies documentation required to be retained, the period of retention and the form in which it must be retained for compliance with taxation law.
Salary sacrifice policy	A policy should be documented outlining employee entitlements as part of salary sacrifice arrangements, in line with legislation. This policy should be reviewed periodically and updated as required in line with any changes to legislation, and communicated to relevant personnel.
Dual authorisation disburse payments	The banking application should require dual electronic authorisation for release of the Electronic Funds Transfer (EFT) file. The ability to authorise payment within the banking application should be segregated from the ability to create a payment within the application. All banking application users should not have the ability to process payroll transactions. In situations where employees are paid bonus payments, such payments should be approved by an appropriate authority. The payroll proposal (if bonuses are calculated by the payroll module) or external schedule (if bonuses are calculated using Excel or a similar package) outlining the bonuses payable should be agreed to the approved methodology.
Automated interface of EFT file to banking application	The EFT file should be stored in a secure network location and the banking application configured to check this location periodically to identify and process any files. Once the EFT file has been successfully released, it should be permanently removed.
Reconciliation of disbursed amount to approved ledger	Authorisers should reconcile the proposed final approved payroll hard copy report (or approved ad-hoc payment documentation) to the amount showing as ready to be disbursed (from the EFT file).
Record, authorise and review benefit plans	Changes to employee benefits should be recorded and approved appropriately prior to the changes being implemented in the HRMIS.

IMPORTANT UPDATE

5. System maintenance and integration

Various functions and configuration options can be used within HRMIS to enhance the control environment or to increase efficiency within HR management processes. The extent of configuration of system controls varies across organisations. Factors such as entity size, size of the HR team, and whether payroll processing is outsourced contribute to the business requirements to operate and configure controls. The chapter provides an overview on 'additional configurable controls' that may contribute to increasing the efficiency of the HR function and may equally contribute to the accuracy of the HR outputs.

5.1 Key control objectives

Control objective	Risks mitigated
Payroll information is completely and accurately posted to the General Ledger via the payroll journal.	**R501:** Payroll system does not reconcile to the General Ledger.
Information regarding superannuation contributions is submitted to superannuation funds (such as ComSuper) via an automated interface, ensuring complete and accurate transfer of data.	**R502:** Incomplete or inaccurate submission of superannuation data.
The rate at which leave accrues and leave types to which employees are entitled is accurately established.	**R503:** Leave accrual rates are established inaccurately.
Fields requiring translation into a foreign currency correctly reference accurate foreign exchange rates within the HRMIS to enable accurate calculations.	**R504:** Employee wages paid in foreign currency are calculated incorrectly.
The organisational chart within the application is continuously maintained to accurately reflect vacant and filled positions within the entity, assisting with position management and recruiting efforts.	**R505:** The HR system organisational chart does not accurately reflect current employees and their position.
Payroll schemas and business processing rules are comprehensively and accurately established to enable a stable payroll calculation requiring minimal manual intervention, and are protected from unauthorised modification.	**R506:** Payroll schemas established or modified inaccurately or without authorisation.
Risks to business systems are generally reduced when available patches are installed in a timely manner after being tested for reliability and usability.	**R507:** Application is vulnerable to security or availability threats.

IMPORTANT UPDATE

5.2 Managing system interfaces

Interfaces to and from the HRMIS present a significant area of risk to maintaining the integrity of HRMIS data. HRMIS data may be exchanged with other internal business systems and changes to one system may affect the integrity of data in another. The integrity and completeness of data transfers or outputs from the HRMIS to external systems may be affected by internal system changes, changes the ICT environment, or changes made by a third party to the external system. As systems and the IT control environment are rarely static, additional manual controls to confirm the completeness and accuracy of data transfer should also be considered.

There are several ways in which information is exchanged between information systems. Agencies may use Enterprise Resource Planning (ERP) systems, which are usually integrated systems using the same software, and may include both financial management and human resource management functions. Integrated systems transfer and update data from one system to the other in 'real time' and often this is automated. Often such systems will have reports or output files that are pre-configured to comply with reporting requirements. A benefit of such systems is that the transfer of information does not require customisation, unless the entity has modified standard system functionality.

Generally, agencies use a HRMIS that is a separate system to other business and financial systems and this will mean that information is shared between systems via an interface. In some cases, agencies may use a payroll processing system that is not integrated with systems that manage employee information. An interface manages the transfer of data from one system to another system. Data transfer may not require manual processing, however, the sharing of information between systems requires careful management to ensure that data is exchanged accurately and completely in a timely manner.

Financial reporting interface

The integrity of financial reporting is of critical importance for Australian Government agencies. Financial reporting is required to be prepared to comply with the Australian Accounting Standards, and the Finance Minister's Orders.[14]

Payroll is a significant expense for most agencies. It is therefore very important that the payroll entries calculated within the payroll system are accurately and completely transferred to the General Ledger within the financial reporting system.

Accurate transfer of payroll results to the General Ledger is via an interface between the payroll system and the financial management system. The posting of payroll results to a General Ledger may not always be automated or integrated into the processing process.

Superannuation payment – Interface with ComSuper

APS agencies are required to report periodically to ComSuper on superannuation deductions for those employees who have a superannuation account with government schemes.[15] ComSuper provides an online superannuation service that enables APS employers to submit, correct and validate superannuation data using a secure online login. Employers are able to use the Payroll Interface File format to transmit relevant data and information from the entity's payroll system to ComSuper.[16] Employers are also able to run individualised superannuation reports through the online superannuation service (ESO) provided by ComSuper, which could include error reports, anniversary salary reports and short-payment reports.

14 For further information on the preparation of financial statements for the Australian public sector, refer to ANAO Better Practice Guide—*Preparation of Financial Statements by Public Sector Entities*, June 2009, Canberra.

15 ComSuper provides superannuation administration services under authority from the Boards of Trustees responsible for the Commonwealth Superannuation Scheme (CSS), Public Sector Superannuation (PSS) scheme, Public Sector Superannuation accumulation plan (PSSap), Military Superannuation and Benefits scheme (MilitarySuper) and the Defence Force Retirement and Death Benefits (DFRDB) scheme.

16 For further information on ComSuper, refer to http://www.comsuper.gov.au. Information regarding the file format is available electronically at http://employer.pss-css.gov.au/your-toolkit/data-reporting/.

IMPORTANT UPDATE

Risks and controls

R501: Payroll system does not reconcile to the General Ledger	
Risk type	
Consequence	The payroll system should reconcile to the General Ledger to ensure integrity of the financial statements. If not reconciled, or reconciled incorrectly, there is an increased risk of material misstatement in the financial statements.
Better practice	**S29:** *Utilise auto-posting functionality.* Where auto-posting functionality is available within the application, it should be utilised to update the General Ledger. Appropriate configuration between the systems is required, and this should be manually triggered so that only final approved payroll results are updated to the General Ledger. **M63:** *Review of payroll posting results.* A review of payroll results that have not posted to the General Ledger should be performed at each pay cycle. If payroll transactions are manually posted (or a file manually uploaded into the General Ledger), a reconciliation should be performed and payroll that is not posted should be actioned.

R502: Incomplete or inaccurate submission of superannuation data	
Risk type	
Consequence	Information submitted to the superannuation fund is incomplete or inaccurate, potentially leading to penalty payments or incorrect reporting of superannuation payments.
Better practice	**S30:** *Superannuation data is provided in the required format and in the required timeframes.* Superannuation data should be provided in the required format and in the required timeframes as defined by the relevant recipient. Where available, the entity should generate such reports and data from the payroll system data. **S31:** *Changes to superannuation interfaces and data file formats are managed using entity IT change management controls.* Changes and upgrades to the HRMIS should not inadvertently modify customised interfaces or data files.

Optimising the control environment

Better practice considerations are highlighted below which should be implemented so that transfer of data from, or received by, the HRMIS is authorised and accurately processed:

Control item	Description
Manual payroll to General Ledger reconciliation	All key payroll module line items (for example, salary cost; deductions) should be manually reconciled to the General Ledger entry to ensure complete and accurate transfer of information. When reconciling files or transactions that are posted to the General Ledger, it is recommended that the individual who initiates the transaction does not perform the reconciliation. The reconciliation should be performed by another employee.

IMPORTANT UPDATE

5.3 Managing system rules

System rules relating to matters such as leave types, foreign currency management, position management and payroll configuration require sound controls to ensure the payroll and HR information is accurately and consistently processed.

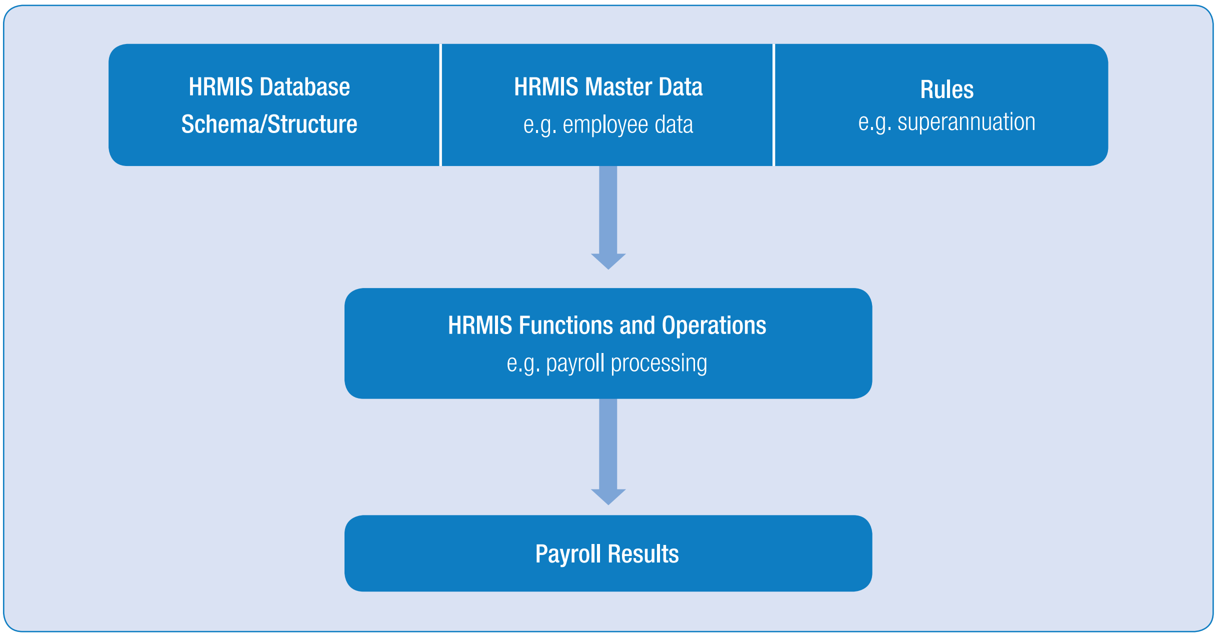
Payroll configuration

Subject to time information being accurately captured, the use of a HRMIS enables a highly automated and accurate payroll calculation. Configured correctly, payroll schemas[17] and rules result in a stable payroll calculation. However, if performed incorrectly they can produce errors which are difficult to rectify.

HR and payroll systems have different database structures and as a result the way in which HR functions and operations are performed differ between HRMIS applications. Understanding the way in which the HRMIS performs payroll functions is important in designing reports, or identifying and fixing processing errors.

The relationship between schemas and other components of payroll processing is illustrated in Figure 5.1:

Figure 5.1: The relationship between schemas and other components of payroll processing



Overview of PeopleSoft, SAP and Aurion HRMIS payroll configuration

Within a PeopleSoft environment, establishment of the Human Resources and Global Payroll Tables is the necessary step to enable an accurate and automated calculation. Further configuration of elements and rules will enable ‘customary’ payroll processing, while specialised elements and rules can assist with meeting legislative superannuation and payroll taxation requirements.

Within the SAP HRMIS application, payroll schemas and rules are the bridge between HR master data and payroll results. A payroll schema specifies payroll functions, with each performing a specific operation (for example, reading data, calculating taxes, processing wage types).

17 In computer programming, a schema refers to the organization or structure of a database and generally defines the structure and content for each data element within the database structure.

IMPORTANT UPDATE

Within the Aurion environment, the People module is the core module. All people are recorded in this module first as a Person, then optionally as an Employee. Aurion assigns a Person Number to all people. This number is different from the Employee Number, which is only assigned when a person is commenced on the Payroll or Leave modules.

The Guide provides further detail on the particular schemas and rules relevant to the PeopleSoft, SAP and Aurion HRMIS payroll configuration.

Leave accruals

Leave accrual rules are based on employee leave entitlements, and the rate at which the leave is accrued. The types of leave accrued and rate at which accrual occurs may be defined by a relevant Award or entity agreement.

There are a number of other factors that affect the accurate accrual of leave:

- Employee's start date—this will influence the long service leave entitlement and other leave entitlements based on the employee's commencement anniversary, (for example, increase in the number of personal leave days); and
- Employee employment type, including whether the employee works full-time or part-time. For part-time employees, leave accrual may require adjustment.

Accounting for long service leave is subject to Accounting Standards and legislation. While recreation or personal leave will typically be accrued using a simple calculation of accrued hours multiplied by employee hourly pay rate, the provision reported in the financial statements for long service leave is a complex calculation based on actuarial calculations of estimated years of service and salary movements.

If system-calculated, leave accrual balances should automatically be posted to the General Ledger on a monthly basis. If manual intervention is required within the calculation, a journal may be posted to update the General Ledger.

Foreign currency

Translation of balances or transactions into foreign currency must be carefully managed to make certain translation utilises the correct rate and follows accounting requirements.

Determination of the foreign exchange rate (FX) to be utilised (for example, spot rate, month end rate) should be determined through consultation with accounting advisers. Implementation of an automated update of FX rates reduces the likelihood of use of incorrect rates in calculations.

Position and organisation structures

Organisational structures are often presented by way of hierarchical diagrams that depict reporting lines between employees, or relationships between internal teams, workgroups and individuals.

There are many different organisational structures, including functional structures, divisional structures and matrix structures.

If the organisational chart is kept current and accurately reflects filled and vacant positions within an entity, it may serve a number of uses. For instance:

- Position management is often able to be linked to the organisation structure in the HRMIS;
- Long and medium term higher duty positions may be documented in the organisational chart, enabling validation when reviewing pay reports;
- Vacant positions within the organisation structure may drive recruiting initiatives;
- Levels and roles within the structure may automatically link to position profiles which in turn link to employee entitlements; and
- Headcount as shown on the structure may enable production of estimated payroll cost reports, which can be compared to actual payroll cost for reasonableness. These reports will also assist in future budgeting for headcount and labour cost.

IMPORTANT UPDATE

Risks and controls

R503: Leave accrual rates are established inaccurately	
Risk type	$
Consequence	Inaccuracies in leave accruals reduce the accuracy and reliability of the payroll calculation and associated financial reports.
Better practice	**S32:** *Manage leave accrual rules.* Leave accrual rules are used to calculate employee leave accruals. The leave accrual rules should be consistent with employee conditions for employment (and/or employee agreement) and linked within the application to employee entitlement information. **S33:** *Configuration of maximum values for leave accruals.* If employee conditions of employment specify a maximum amount of leave which can be accrued or carried forward, maximum values should be configured for each type of leave accrual. If the maximum leave accrual amount is reached, an error message should be reported and the system designed to stop accruing further leave. **M64:** *Regular review of employees' leave accruals should be performed.* A manual review of employee's leave accruals should be performed by managers to assess for reasonableness against known periods of leave taken by employees. A further review should be performed by HR to identify any excessive or negative balances.

R504: Employee wages paid in foreign currency are calculated incorrectly	
Risk type	$
Consequence	Use of inaccurate foreign exchange rates for currency translation purposes will result in inaccurate calculation of payroll.
Better practice	**S34:** *Establish automated updates for foreign exchange rates.* An automated update of foreign exchange rates should be established with an authorised source and the entity application to ensure rates applied are up to date and accurate.

IMPORTANT UPDATE

R505: The HR system organisational chart does not accurately reflect current employees and their positions	
Risk type	
Consequence	Incomplete organisation chart may impair the accuracy of workflows associated with self-service functionality, and user access privileges. Other impairments include headcount errors and incorrect workforce planning decisions.
Better practice	**S35:** *Restricted access to update organisational chart.* Access to update the organisational chart should be restricted to appropriate personnel. Amendments should only be processed based on appropriately approved documentation (for example, authority to create a new position). **S36:** *Ability to display temporary assignments.* Functionality enabling the organisational chart to display temporary assignments should be utilised to enable tracking of higher duties assignments. **S37:** *Organisational chart designed to reflect the hierarchy.* The organisational chart should be designed to reflect the hierarchy for each department or organisational unit.

R506: Payroll schemas established or modified inaccurately or without authorisation	
Risk type	
Consequence	Payroll accuracy is impacted as a result of errors caused by the incorrect set-up of payroll schemas or rules that cause the schemas to execute calculations inaccurately.
Better practice	**S38:** *Access to establish or modify payroll schemas or elements and rules is restricted.* Access to set up or modify payroll schemas or elements and rules should be restricted to appropriate personnel.

IMPORTANT UPDATE

Optimising the control environment

Better practice considerations for managing system rules are highlighted below:

Control item	Description
Change management controls over payroll configuration	All developed schemas/elements/rules should be tested to validate they operate in accordance with the design. This testing should take place outside of the 'live' payroll environment. Change management controls should be implemented over any changes to payroll configuration to ensure the change is appropriately approved and that the configuration change complies with regulations and legislation.
Managing changes to system rules	An automated trigger designed in the application or a manual trigger prompted by a checklist should be established to manage changes to employee circumstances which would affect leave accruals, and result in the change to leave accruals being processed. These changes could include changes to entitlements, changes to work status (for example, full-time to part-time employment), or a period of leave without pay during which entitlements are not accrued. Prior to performing a pay run, a test should be performed to confirm leave is accruing accurately in line with the changed information, and a check should be undertaken to ensure changes were appropriately approved.
Independent verification of manually keyed foreign exchange rates	If an automated update is not possible and foreign exchange rates must be keyed manually, the rates keyed should be verified for completeness and accuracy.
Periodic review of salary/wage payments made in foreign currency	A periodic review should be undertaken of all employees paid in foreign currency to determine whether the amounts paid are consistent with contractual terms and whether any adjustment is required if a fixed foreign exchange rate has been stipulated in the contract. Any adjustment should be appropriately approved before being updated in the application. The rate established for translation should be independently verified for accuracy against approved documentation. Fluctuations in payment amounts should be reviewed for reasonableness as a component of the review of the payroll proposal.
Periodic review of HRMIS organisational chart	A manual review of the organisational chart should be performed by managers to determine whether it accurately reflects the team structure, including any higher duties currently being performed within the team. An overall review should be performed by HR against a listing of all employees and termination, transfer and new engagements listings to confirm the organisational chart reflects current employees within the entity.

IMPORTANT UPDATE

5.4 Managing software updates

A software update generally refers to an update of a computer program or its supporting reference data by a software vendor. This includes fixing security vulnerabilities and improving the usability or performance of the program. Software updates may either be at the operating system, database or application level. Often designed to fix problems, poorly designed software updates can sometimes introduce new issues, particularly where elements of the HRMIS (such as reports) have been customised.

Risks and controls

R507: Application is vulnerable to security and availability threats	
Risk type	
Consequence	A software update is not installed in a timely manner or not installed completely and accurately, making the application vulnerable to security breaches and threatening the availability of the application.
Better practice	**S39:** *Automatic notification of available software updates.* Automatic notification should be configured to alert the system administrator whenever a software update is available. **M65:** *Timely installation of approved software updates.* All software updates should be tested in a controlled environment (replicating the production environment) before being released into production.

Optimising the control environment

Establishing an effective control environment is critical to ensuring that HR information and processing is accurate and complete and that the integrity and confidentiality of information is maintained. Undetected weaknesses in the processes and controls that manage the information technology control environment may reduce the effectiveness of HRMIS controls.

The following better practice guidance may be of assistance in determining the effectiveness of important controls in the IT environment.

Change Management

Effective change management controls are important to ensure that changes are authorised and appropriately tested before being introduced into the production system. Change management weaknesses may impair the proper classification and reporting of HR expenses and may reduce the integrity of information contained in employee records.

A change management process should be maintained for the HRMIS. The change management process should also prevent changes being made to employee data, payroll reference data and its configuration without appropriate authorisations, such that:

- all requests for changes to the HRMIS application or changes to the underlying database structure should be reviewed and approved by the HR head prior to being implemented;
- all changes should be adequately tested prior to being implemented in the production environment. The testing process should include tests of the integrity of data exchange with other internal applications (such as the financial management system) and exchange of information with external IT systems and interfaces (such as the periodic transfer of superannuation information to ComSuper or other superannuation funds); and
- segregation of duty controls should be implemented to restrict the ability of staff to make system changes in both the production database and the configuration of the HRMIS software.

IMPORTANT UPDATE

Due to the criticality of the HRMIS and time-sensitive aspects of its operations (payroll processing, contributions etc), application maintenance and upgrades should be incorporated into the change management process. Timely implementation of software updates for the HRMIS is important as such updates often include changes resulting from taxation and superannuation legislation.

Management of the implementation of software updates should:

- assess the source of the update (for example, updates should only be accepted from authorised distributors);
- test the implementation of the update in an environment separate to the production system to determine whether system performance will be impacted;
- include user acceptance testing following installation of the update in a test environment; and
- include documentation of a 'roll-back plan' that describes the process required to restore the application and database settings to its previous state.

Interface Management

Interfaces to the HRMIS present a significant area of risk to maintaining the integrity and confidentiality of HR information. Interfaces include the internal interface to the General Ledger and other business systems. External interfaces may include interfaces to ComSuper and the Australian Taxation Office. Refer to section 5.2.

Employee and payroll information that may be transmitted and received through interfaces to the HRMIS requires system managers to implement controls that manage and control configuration changes to the interfaces. System changes should be approved and tested prior to implementation to reduce the risk of errors occurring.

Additionally, implementing manual controls using reporting from the HRMIS to reconcile transactions may assist the HR practitioner to confirm the completeness and accuracy of data transfer.

User Access Management

Effective user access management controls provide assurance that HR systems are appropriately secured to prevent unauthorised use, disclosure, modification or loss of data. User access management is also a critical component in providing effective segregation of duties, such that:

- access or changes to access privileges should be approved and documented;
- users of the HRMIS should be uniquely identifiable. Users should have an individual access identifier and not 'share' passwords;
- administrator access or 'privileged' access should be limited within the HR team;
- system access should be based on user roles'— HR Manager, Line-Manager, etc; and
- system access privileges and business rules should comply with segregation of duty requirements.

Business Continuity Management

The maintenance of any system requires considerations of steps that would be taken should interruption be experienced in the function of the system. With numerous compliance and legislative requirements relevant to the HR and payroll processes, agencies must be confident that they have procedures in place to recover from such interruption, such that:

- agencies should have a documented strategy for management of the cyclical backup of HR data and programs;
- retention periods and storage requirements for HR data, messages, reports and output files should be defined; and
- requirements should be identified and implemented for the protection of sensitive information and to safeguard against the unauthorised disclosure or modification of sensitive HR information.

IMPORTANT UPDATE

IMPORTANT UPDATE

Human Resources Management Information Systems – Risk and Controls

Better Practice Guide

Part 2
System-specific Controls

IMPORTANT UPDATE

IMPORTANT UPDATE

6. PeopleSoft – Human Capital Management

The chapter examines the risks and controls as applied to the Oracle PeopleSoft Enterprise human capital management module—and applies to releases 8.9, 9.0 to 9.2.

6.1 PeopleSoft controls for HR and payroll data management

Employee information may be stored as 'standing' master data—which is drawn upon by nearly every activity in the payroll process, including time entry, payroll processing and benefits administration—or as information capture subject to regular change and update, such as performance management and time reporting. The nature of such information is sensitive and subject to privacy and legislative requirements and therefore should be adequately controlled.

The PeopleSoft application controls access to HR and Payroll data via a combination of configuration settings and user access controls. Configuration settings include controls configured when initially installing the application. Configuration controls such as appropriate default master data field value settings, TableSets and SetIDs are an important component of setting up and restricting master data access based on organisational requirements. Validation keys are another important configuration item that helps prevent duplicate field values for sensitive data capture fields such as tax file number, via the use of the Search/Match functionality of PeopleSoft. User access controls implemented via permission lists and roles help restrict access to HR and Payroll master and transactional data according to organisational requirements. Consideration should also be given to default permission lists and PeopleSoft roles such as the PeopleSoft Administrator role and PSADMIN permission list which provide overarching access to HR and Payroll data within PeopleSoft.

Key control objectives

Control objective	Risks mitigated
HR and payroll data is appropriately maintained to provide accurate and complete employee information and payroll transactions.	**R201:** HR master data is inaccurate. **R202:** HR master data is not secure.

IMPORTANT UPDATE

Risks and Controls

R201: HR master data is inaccurate	
Risk type	
Consequence	Employee details may be incorrectly entered or maintained, which may result in duplicate payments, errors with superannuation contributions or employee deductions, or unapproved changes to the allocation of roles and delegations.
Better practice	**S01:** *Define key data entry fields.* Key data fields should be defined in the system to confirm that information necessary to the completion of master data is entered. The installation configuration of PeopleSoft defines the various default values for data entry that are configured within the application. These configuration items can be undertaken on specific data elements within PeopleSoft as follows: • Company code, default hours (minimum, maximum, standard), work periods, compensation frequency, position management parameters, currency settings, automatic termination, suspensions, field length and configuration for default settings for key HRMIS IDs such as employee ID, and default system numbering parameters. A method to review the values configured is via the PER702 Installation Table Report (Path – Set Up HRMS, Install, Installation Table Report) that outlines the default field and data values that have been set up. • Business Units – logical units within the entity's organisation. This could be set up as agencies, subsidiaries, divisions, or branch offices as appropriate for the entity's purpose. A method to review these values is via Path – Set Up HRMS, Foundation Tables, Organisation, Business Unit and Path – Set Up HRMS, Foundation Tables, Organisation, GL Business Unit. • Location – configuration values for physical locations within the entity (headquarters, branch offices, satellite offices etc). A method to review these values is via the Location Table Report PER705. • Company – entity related information including tax and payroll information. Review these values via (Path – Set Up HRMS, Foundation Tables, Organisation, Company Table Report) which provides company specific information that has been configured. • Departments – configuration values for departments/cost centres that have been configured within the entity/locations. A method to review the values configured is via Path – Set Up HRMS, Foundation Tables, Organisation, Department Table Report. • TableSets and SetIDs – TableSets refer to default data values to be shared across all business units – for example, job codes, positions and so on. SetIDs enable the sharing of these data values as configured within permission lists. PeopleSoft utilises TableSets and SetIDs to organise and control the manner in which stored data is accessed via the application and segregated in terms of data access. The use of TableSets and SetIDs helps the entity to segregate access to HRMIS data based on organisational needs. In a large entity, the use of TableSets and SetIDs can help to appropriately segregate HRMIS data within the various organisational units of the entity. TableSets and SetIDs can be accessed via the following path – (Path – PeopleTools, Utilities, Administration, TableSetIDs). • A related consideration is to determine field validation key configuration at the database level. Appropriate configuration of validation keys helps to prevent duplicate field values for sensitive data capture fields such as tax file number, via the use of the Search/Match functionality of PeopleSoft.

IMPORTANT UPDATE

R201: HR master data is inaccurate	
	• Default data values/Permission list – configuration values for default items such as minimum/maximum working hours, company codes, work period and compensation frequency, settings surrounding automatic termination, suspensions. A method to review the values configured is via (Path – Set Up HRMS, Foundation Tables, Organisation, Org Defaults by Permission List • Job and Payroll management configuration – configuration values on workforce and payroll configuration values which include employee type, salary bands, currency and frequency. Configuration values can be obtained from reports PAY711, PAY717 and PER709C. In addition, PeopleSoft is installed with Departmental Security configured as default. Departmental Security ensures that users are only able to access employee data linked with their Departmental ID. This would be a key concern primarily for larger agencies where cross-departmental access may be required for a shared services HR function. (To review – (Path – Set Up HRMS, Security, Department Security, Security Tree Audit Report) Configure the Supporting Documents Table (Path – Set Up HRMS, Common Definitions, Supporting Documents) so that additional employee master data information (such as personal details, previous employment history, educational and professional qualifications and so on) can be entered. Configure checklists to obtain standard sets of data to consistently capture master data sets for all new employees (Path – Set Up HRMS, Common Definitions, Checklists, Checklist). **S02:** *Restricting user access to view, establish and update master data.* Access to view, establish and update master data should be restricted to appropriately authorised users. Users with the ability to view master data should also be appropriately restricted to reduce the likelihood of inappropriate viewing or distribution of data. 1. Access to the following employee master record tables should be appropriately restricted: • PS_EMPLOYMENT – this table contains key employment data such as hire/rehire date, probation date, pay increase information, length of service, termination date, last day worked. • PS_PERSON – this table contains all current and historical personal data about an employee such as ID, name, address, phone number, citizenship status, hire date, and so on. Review changes made to critical tables via the PER029 Database Audit Report (Path – Workforce Administration, Workforce Reports, Database Audit) to determine if changes made have been undertaken by authorised personnel. 2. Review access to permissions lists and roles that have access to maintain the master record tables. This can be done by reviewing information extracted from the following tables: • PSAUTHITEM – Provides details on permission lists that have been configured/enabled. Work with the PeopleSoft Administrator to determine the permission lists that have been customised which provide access to maintain the master data tables. • PSROLECLASS – Provides details on permissions that are linked to roles. Information from this table will enable the determination of the roles that have the permission lists identified above which will help in determining users with such access.

IMPORTANT UPDATE

R201: HR master data is inaccurate	
	• PSROLEUSER – Provides details on roles linked to user profiles. Information from this table will identify users who have access to maintain the master record tables. • PSOPRCLS – Provides details on permissions linked to user profiles. Information from this table will identify users who have the relevant permission lists assigned directly to their user profiles. 3. In addition to the customised permission lists and roles identified in (2) above, access to standard PeopleSoft roles and permission lists should also be reviewed for usage as these default security items have powerful access and will allow for access to the master record tables. Access to these roles and permission lists should be restricted as the norm. **S03:** *Validation checks on certain fields warn the user that the information is duplicated in another employee record.* Validation checks should be configured to decrease the likelihood of inaccurate information being entered (for example, tax file number cannot be duplicated in another employee record). **Field validation** checks are configured as part of the installation of the application. Appropriate configuration of validation keys reduces the likelihood of duplicate field values for sensitive data capture fields such as tax file number, via the use of the Search/Match functionality of PeopleSoft. A method to review the values configured is via the PER702 Installation Table Report (Path – *Set Up HRMS, Install, Installation Table Report*) that outlines the default field and data values that have been set up. **Personnel Actions** is a configurable element that relates to reason codes for changes to personnel data. Appropriate configuration of this element helps the entity keep track of the rationale for potential changes that can be undertaken on employee data. The values configured are stored in the Action Reason Table (Path- Set Up HRMS, Product Related, Workforce Administration, Action Reasons). Review the **Action Reason Table Report (PER710)**. This report lists the reason codes for each personnel action code. **M50:** *Establishment and amendment of master data occurs only when supported by appropriately approved documentation.* All master data established and all amendments processed to master data should be supported by appropriate documentation (approved by an appropriate authority where relevant). Reports: PER707 – overview information of companies that have been configured; PER701 – overview information on departments that have been configured; PAY711 – overview information of all paygroups and related characteristics that have been set up; PER709 – overview information of workforce job codes and characteristics that have been set up; PER710 – master data change action/reason codes; and PER029 Database Audit – audit report on changes made to specific tables

IMPORTANT UPDATE

R202: HR master data is not secure	
Risk type	
Consequence	Unauthorised users may have access to view and maintain sensitive HR and payroll data, which may compromise the confidentiality of personnel records and may also result in the processing of fraudulent payroll payments.
Better practice	**S04:** *Access to HR master data is appropriately configured and managed.* Implementing appropriate user access controls requires: • Identification and implementation of segregation of duty requirements in relation to validating updates/modification/deletion of master data within the HRMIS is complete and appropriately authorised; • Access to the application and to underlying data (such as the database) is assigned based on user profiles and/or roles; and • Employees should be limited in their ability to modify reference data items (salary, leave records and employment date) for their own records. With Web Client applications – like employee self-service (ESS) – the client may allow an employee to be able to modify their own data with the exception of high-risk data fields, including salary, hourly rate, additional pay, job grade. Access controls provide appropriate restrictions to user access to certain data types. Access should be controlled at three levels: • Restrict access to appropriate users (for example, HR personnel but in some situations access may be wider if ESS is implemented); • For each authorised user, restrict access to particular types of master data (for example, only some authorised users will have access to bank details); and • For each user and each type of data, specify whether access is 'view' or 'edit' access. Permission lists and roles defined for the agency will provide the controls noted above *S02: Restricting user access to view, establish and update master data is also relevant.* **M51:** *Review of system configuration reports.* Generally system configuration change reports are available from the HRMIS and may be reviewed periodically to monitor changes to key controls or configuration settings. Such reports should be run periodically. Consideration should be given to ensuring that appropriate 'audit' tables and associated logs are also configured. Failure to configure such tables may mean that important information is not available for inclusion in monitoring reports. Reports: • PER029 – Provides an audit trail of changes made to critical tables • PER702 Installation Table Report – outlines the default field and data values that have been set up

IMPORTANT UPDATE

6.2 PeopleSoft controls for workforce management

Key control considerations in PeopleSoft that relate to workforce management include implementing appropriate user access security settings as well as appropriate configuration control settings that are line with legislation and compliance requirements. User access controls implemented via permission lists and roles helps monitor whether access to workforce management is restricted according to organisational requirements. Consideration in this aspect should also be given to default permission lists and PeopleSoft roles such as PeopleSoft Administrator and the HR Administrator role and the HCCPHR30AU and HCCPHR33AU permissions lists which provide overarching access to workforce management functionality within PeopleSoft. From a configuration perspective, workflow configuration for on-boarding and terminating employees is a key control consideration as well as appropriate configuration of job and payroll settings in line with organisational requirements.

Key control objectives

Control objective	Risks mitigated
Appropriate and accurate employee information is collected and maintained.	**R301:** Non-existent or duplicate employee is added to the payroll. **R302:** Termination payments and balances are inaccurately calculated. **R303:** Employee is not deactivated when employment is terminated.

Risks and Controls

R301: Non-existent or duplicate employee is added to the payroll	
Risk type	
Consequence	'Ghost' or duplicate employees on the payroll lead to overpayment or processing of fraudulent payments.
Better practice	**S05:** *Access to add an employee should be restricted to appropriate individuals and segregated from payroll maintenance.* Access to modify employee information should be restricted to decrease the likelihood of inappropriate or unapproved changes to employee information which may impact upon the accuracy and completeness of information maintained in the HRMIS. Additionally, restricting access in accordance with privacy principles reduces the risk of inappropriate disclosure of employee information. 1. Review access to permissions lists and roles that have access to add employees. This can be done by reviewing information extracted from the following tables: • PSAUTHITEM – Provides details on permission lists that have been configured/enabled. Work with the PeopleSoft Administrator to determine the permission lists that have been customised which provide access to add employees. • PSROLECLASS – Provides details on permissions that are linked to roles. Information from this table will enable the determination of the roles that have the permission lists identified above which will help in determining users with such access. • PSROLEUSER – Provides details on roles linked to user profiles. Information from this table will identify users who have access to add employees. • PSOPRCLS – Provides details on permissions linked to user profiles. Information from this table will identify users who have the relevant permission lists assigned directly to their user profiles.

IMPORTANT UPDATE

R301: Non-existent or duplicate employee is added to the payroll	
	2. In addition to the customised permission lists and roles identified in (1) above, access to standard PeopleSoft roles and permission lists should also be reviewed for usage as these default security items provide for an elevated level of user access and will allow for access to add employees. Access to these roles and permission lists should be restricted as the norm. Default roles: • HR Administrator • PeopleSoft Administrator Permissions Lists: HCCPHR30AU: Administer Workforce Set up HCCPHR3320: Hire Workforce HCCPHR33AU: Administer Workforce HCCPSS1020: Benefits-Employee HCCPSS1030: Compensation-Employee HCCPSS1060: Personal Information-Employee HCCPSS1070: Personnel Actions-Employee HCCPSS1400: Employee Personnel Information HCCPSS1200: Employee Data PSADMIN: PeopleSoft Administrator *Also refer to* **S03:** *Validation checks on key fields warn the user that the information is duplicated in another employee record.* 3. A supplementary control to (1) and (2) above is to review changes made to the workforce maintenance tables via the *PER029 Database Audit Report (Path – Workforce Administration, Workforce Reports, Database Audit*) to check that changes are made by approved personnel and changes made are duly authorised. **M52:** *When adding a new employee, a listing of current employees should be reviewed to reduce the risk of duplicating the employee record.* A system report of all current employees should be generated prior to adding a new employee, and checked to confirm the employee does not already exist in the system. A system report of all new employee additions should be generated monthly and an individual who is independent from the employee set-up process should check each addition against supporting paperwork (for example, approval to engage, employee information including bank account) to validate the set-up was authorised and has been completed accurately. Report: PER081 – The Employee listing report lists all employees as at a selected date (by employee name, ID and Department).

Part 2: System-specific Controls

IMPORTANT UPDATE

R302: Termination payments and balances are inaccurately calculated	
Risk type	
Consequence	Termination payment is incorrect, resulting in incorrect salary and leave entitlements being paid or reported
Better practice	**S06:** *Application will warn user if termination date in the past is entered.* The system should be configured such that if a termination date in the past is entered, a warning message is generated to reduce the occurrence of backdating of terminations and to accurately process termination payments and calculations. Invalid date fields to prevent post-dating of terminations are a configuration check that is set up at the installation configuration settings (Path – *Set Up HRMS, Install, Installation Table Report (PER702)*. An error message will prevent the user from backdating the termination date. **S07:** *Workflow operates to require independent approval verification of termination date entered.* Automated workflow approvals utilising organisation hierarchy positions delegations of authority should be utilised to approve terminations. The approver should verify the termination date of the employee prior to approving. Workflow for the termination process should be configured within the HRMIS. Access PeopleSoft Application Designer (system utility) to determine the workflow settings that have been configured for the termination workflow. The workflow Rules should be configured such that terminations are required to be approved prior to being processed within the system and the Roles will determine the appropriate users who have been tasked with the approval responsibility. (Path – *Set Up HRMS, Common Definitions, Self Service, Workflow Status*) **S08:** *Application automatically calculates payments based on master data, termination date entered, and leave entitlements.* Use of system functionality to calculate and report entitlements and balances is more accurate. The effectiveness of this control requires accurate data entry and maintenance of employee information and master data. Payroll and compensation elements are preconfigured within PeopleSoft and enable appropriate calculation of payroll and leave entitlements in the event of a termination. Values of elements configured for the organisation should be reviewed in conjunction with the PeopleSoft Administrator for appropriateness of values in line with organisation requirements. (Path – *Set Up HRMS, Product Related, Global Payroll, System Settings, Element Types*). Some examples of the elements to review are as follows: Default PeopleSoft termination formula TER FM TERM CHECK checks on the termination date against pay period to determine the payout amount. Leave balance entitlement element – AL MARGIN DY. Termination Payment element – TERM LUMP. **M53:** *An independent authority checks the termination date per notification documentation to the date entered in the system.* On a monthly basis, a report of all terminations is generated and an individual who does not have access to terminate employees checks that all termination dates were accurately entered, with reference to termination documentation (for example, resignation letter).

IMPORTANT UPDATE

R303: Employee is not inactivated when employment is terminated	
Risk type	
Consequence	Employee record is not flagged as terminated which may result in subsequent payment to the employee. For agencies using 'single sign on' (which enables access to all applications without requiring separate passwords, by using credentials at the network sign-on level), failure to inactivate terminated employees may also fail to inactivate network access.
Better practice	**S09:** *Application automatically changes status of employee to 'terminated' as at termination date entered.* Systems are configured to automatically change the status of employees to 'terminated' as at the entered termination date. This is typically enabled through automated batch processing. PeopleSoft will automatically update the employee status as terminated upon the termination date. Review reports Personnel Actions History report (PER015) and Personnel Actions Pending report (PER021) to check that terminated employees have been assigned the appropriate 'Terminated' reason code. **S10:** *Application automatically disables terminated employee's access to systems based on termination date entered.* This control is possible where position-based security is utilised. Appropriate use of the termination date is important where single-sign access is granted based on a commencement or termination date. Default PeopleSoft functionality does not enable this. **S11:** *Application does not allow payment to be disbursed to employees with 'terminated' status.* Operation of this control typically does not require specific configuration within the system, as it is deemed 'standard' functionality. It may be possible in some circumstances to process ad-hoc payments to terminated employees using some applications The termination date captured in the system is treated as the day the termination starts and the employee is paid up until the day before. **M54:** *Department/Cost Centre managers are periodically provided with a listing of employees for which they are responsible. This listing is checked to determine whether it contains any employees no longer working within the department.* System generated listings of current employees per department/area/cost centre should be provided to relevant managers to verify current employees. This check assists in detecting employees who have transferred or been terminated and information regarding the transfer or termination has not been recorded in the system. Report: PER801 – overview information of employee name, employee ID by Department.

IMPORTANT UPDATE

6.3 PeopleSoft controls for payroll processing and administration

Key control considerations in PeopleSoft that relate to payroll processing and administration include implementing appropriate user access security settings as well as appropriate configuration control settings that are in line with legislative and compliance requirements. User access controls implemented via permission lists and roles help monitor whether access to payroll processing and administration is restricted according to organisational requirements. Consideration in this aspect should also be given to default permission lists and PeopleSoft roles such as PeopleSoft Administrator, Payroll Administrator and GP Administrator roles and HCCPSS1035 and HCCPGP1 permissions lists, which provide overarching access to payroll processing and administration functionality within PeopleSoft. From a configuration perspective, appropriate configuration of Payroll settings in line with organisational requirements as well as restricting access to core payroll master tables such as GP_RSLT_ERN_DED and PS_ADDL_PAY_DATA is required.

Key control objectives

Control objective	Risks mitigated
Evidence of employee service and time is accurately recorded in the appropriate period.	**R401:** Inaccurate or incomplete entry of employee time data. **R402:** Unapproved leave or leave is taken outside of entitlements. **R403:** Established employee shifts are updated inaccurately. **R404:** Time recorded in prior periods is amended inaccurately or without appropriate authority.
Evidence of employee service and time is accurately recorded in the appropriate period.	**R405:** Payroll calculation is inaccurate or incomplete.
Evidence of employee service and time is accurately recorded in the appropriate period.	**R406:** Statutory obligations for payment of taxation are breached. **R407:** Breach of legislative requirements relating to superannuation. **R408:** Salary sacrifice arrangements are not appropriately managed.
Evidence of employee service and time is accurately recorded in the appropriate period.	**R409:** Methodology for bonus rewards is not established. **R410:** Employee benefits are not managed or administered in accordance with Workplace Agreements/employee contracts.

IMPORTANT UPDATE

Risks and controls

R401: Inaccurate or incomplete entry of employee time data	
Risk type	
Consequence	Time data entered does not accurately reflect time worked or does not include leave taken. Employee receives payment for hours or leave to which they are not entitled.
Better practice	**S12:** *Workflow approval of employee time.* Where workflow functionality is used, such as in self-service, the workflow should be configured so that submitted employee time is automatically routed through the workflow approval hierarchy for review by the employee's immediate supervisor or functional manager. The workflow should also be used to send rejected time allocations or leave requests to the employee via the system with the reason recorded. Workflow for timesheet approvals should be configured within the HRMIS. The workflow Rules should be configured such that users are not able to approve their own time and the Roles will determine the appropriate users who have been tasked with the approval responsibility. Approval responsibility which will typically be in line with the organisational structure or an approver may be responsible for certain groups of employees. Review System Workflow Rules (Path – *Set Up HRMS, Common Definitions, Self Service, Workflow Status*). **S13:** *System validation of data entered.* Validation checks should be configured to decrease the likelihood of inaccurate time being entered (for example, minimum/maximum number of working hours, checks against established time codes). The system may also be configured to provide default timesheets to employees with standard responsibilities and working hours. PeopleSoft enables the creation of work schedules which specify expected working hours, non working hours (holidays etc). (Path – *Set Up HRMS, Product Related, Time and Labor, Schedules, Workdays* and Path – *Set Up HRMS, Product Related, Time and Labor, Schedules, Definitions*). The schedules defined can be reviewed from an appropriateness perspective via Path – *Set Up HRMS, Product Related, Time and Labor Schedules, View Schedule Calendar*. **S14:** *Timesheets are locked for editing after submission.* After submission, the system should restrict employees from being able to edit time submitted. In order to alter time, a prior period adjustment must be processed. Row Security permission lists within PeopleSoft can be configured to restrict users from making prior period adjustments. Row Security Permission lists configured can be determined via Path – *Set Up HRMS, Security, Time and Labor Security, TL Permission List Security*. Users who have been granted such permissions can be reviewed via Path – *Set Up HRMS, Security, Time and Labour Security, TL Permission List Security, Row Security Users*. **S15:** *Automated notifications.* Automated notifications remind users to enter their time report, and continue to alert users when the time reporting deadline is reached and passed. Employee notification for the workflow is configured as part of the workflow rules (Path – Set Up HRMS, Common Definitions, Self Service, Workflow Status).

IMPORTANT UPDATE

R401: Inaccurate or incomplete entry of employee time data	
	M55: *Review 'Missing Time' report.* Immediately after the time reporting deadline, the payroll department should generate a report outlining missing time and follow up directly with employees and the employees' functional managers. PeopleSoft enables the management of missing time or missing timesheets as Exceptions. Path – *Set up HRMS, Product Related, Time and Labor, Approvals, Manage Individual Exceptions*. Report: TL001 – report which provides time entered by employee name, ID and work date.

R402: Unapproved leave or leave is taken outside of entitlements	
Risk type	
Consequence	Employee takes leave which is either not recorded on timesheets, or when recorded results in the employee having a negative leave balance.
Better practice	**S16:** *Automated checks on leave applications to confirm sufficient entitlement.* Use of system functionality to capture leave requests will enable comparison reporting to be generated and show any discrepancies between leave recorded in timesheets and leave requested. Leave balances are maintained by Leave Plan Table (LEAVE_PLAN_TBL) and Leave Accrual Table (LEAVE_ACCRUAL) of the Benefits system to validate time reported via time reporting codes (for leave) against the availability of leave. Configuration of negative leave balances is enabled via the Leave Plan Table. PeopleSoft functionality for the calculation of availability of leave takes into consideration unprocessed hours taken (applied). **S17:** *Workflow approval of leave requests.* System functionality to process leave requests (for example, Employee Self Service) should be utilised to enable automated checks to be performed against employee entitlements and leave balances. Requested leave should route through the workflow approval hierarchy for approval prior to the request being approved. The application should be configured to raise a 'warning flag' if the requested leave will result in negative entitlement balances. Workflow for leave approvals should be configured within the HRMIS. The workflow Rules should be configured such that users are not able to approve their own leave and the Roles will determine the appropriate users who have been tasked with the approval responsibility. Approval responsibility, which will typically be in line with the organisational structure, or an approver, may be responsible for certain groups of employees. Review System Workflow Rules (Path – *Set Up HRMS, Common Definitions, Self Service, Workflow Status*). **M56:** *Periodic review over recording of leave.* A two-way check should be performed by the payroll team on a monthly basis to confirm that: • Leave taken by employees in reflected in timesheets; and • Leave recorded was appropriately approved. Any discrepancies should be followed up with the employee and the employee's immediate supervisor. Report: GPAUAM02 – overview report which provides leave accrual information by employee. The report outlines eligible hours, leave taken to date and remaining leave balances.

IMPORTANT UPDATE

R403: Established employee shifts are updated inaccurately	
Risk type	
Consequence	Inaccurate employee shifts reporting may lead to inaccurate payroll processing and may impact leave accrual calculations.
Better practice	**S18:** *Restrict user access to amend employee shifts.* Access to update employee shifts should be restricted to appropriate personnel and employees should not have access to update their own shift details. PeopleSoft enables the creation of work schedules or rosters which specify expected working hours, non-working hours (holidays etc). (Path – *Set Up HRMS, Product Related, Time and Labor, Schedules, Workdays* and Path – *Set Up HRMS, Product Related, Time and Labor, Schedules, Definitions*). The schedules defined can be reviewed from an appropriateness perspective via Path – *Set Up HRMS, Product Related, Time and Labor, Schedules, View Schedule Calendar*. Row Security permission lists within PeopleSoft can be configured to restrict users from making adjustments to works schedules. Row Security Permission lists configured can be determined via Path – *Set Up HRMS, Security, Time and Labor Security, TL Permission List Security*. Users who have been granted such permissions can be reviewed via Path – *Set Up HRMS, Security, Time and Labour Security, TL Permission List Security, Row Security Users*. **M57:** *Approval of updates to employee shifts.* Employee shifts should only be updated in the system following approval by an appropriate authority. Report: TL004 – provides an overview on scheduled hours by employee which allows for the identification of anomalies to employee work schedules which can subsequently be followed up for approval and authorisation.

Part 2: System-specific Controls

IMPORTANT UPDATE

R404: Time recorded in prior periods is amended inaccurately or without appropriate authority	
Risk type	
Consequence	Inaccurate or unauthorised adjustments lead to inaccurate leave balances or time reporting.
Better practice	**S19:** *Restrict user access to process prior period adjustment.* Access to process prior period adjustments should be restricted. This may require a procedure to be put in place whereby a manual request (appropriately approved) is submitted. Row Security permission lists within PeopleSoft can be configured to restrict users from making prior period adjustments. Row Security Permission lists configured can be determined via Path – *Set Up HRMS, Security, Time and Labor Security, TL Permission List Security*. Users who have been granted such permissions can be reviewed via Path – *Set Up HRMS, Security, Time and Labour Security, TL Permission List Security, Row Security Users*. **S20:** *Workflow approval of prior period adjustments.* Amendments to time recorded in prior periods should be processed through the workflow approval hierarchy. Workflow configuration rules can be configured to limit access to specific roles/approvers that can make prior period timesheet adjustments (Path – *Set Up HRMS, Common Definitions, Self Service, Workflow Status*). **S21:** *Limit prior period adjustments.* The system should limit the prior period for which adjustments can be processed (e.g. four weeks, or a small number of immediate past periods). Row Security permission lists within PeopleSoft can be configured to restrict users from making prior period adjustments and to limit the number of periods into the past within which adjustments can be processed. Row Security Permission lists configured can be determined via Path – Set Up HRMS, Security, Time and Labor Security, TL Permission List Security. **M58:** *Approval of prior period adjustments prior to processing.* When a prior period adjustment is required, the details are documented on a standard form requiring approval from an appropriate authority prior to processing. The adjustment is then processed in the system by a member of the payroll team. **M59:** *Review prior period adjustments.* On a monthly basis, a report should be generated that lists all prior period adjustments processed. This report should be reviewed to determine the appropriateness of adjustments processed. Report: While there is no standard report within PeopleSoft for prior period adjustments, PeopleSoft allows for prior period adjustments to be reviewed online on an employee by employee basis. An ad-hoc report can be developed.

IMPORTANT UPDATE

R405: Payroll calculation is inaccurate or incomplete	
Risk type	
Consequence	Draft payroll proposals are not reviewed for reasonableness prior to finalisation of the payroll, resulting in failure to detect significant anomalies or errors.
Better practice	**S22:** *Restrict changes and user access to modify payroll calculation rules.* Personnel calculation rules are used to calculate gross and net pay for employees and should be protected from being overridden or modified without appropriate authorisation. 1. Review access to permissions lists and roles that have access to modify payroll calculation rules. This can be done by reviewing information extracted from the following tables: • PSAUTHITEM – Provides details on permission lists that have been configured/enabled. Work with the PeopleSoft Administrator to determine the permission lists that have been customised which provide access to modify payroll calculation rules. • PSROLECLASS – Provides details on permissions that are linked to roles. Information from this table will enable the determination of the roles that have the permission lists identified above, which will in turn help in determining users with such access. • PSROLEUSER – Provides details on roles linked to user profiles. Information from this table will identify users with access to modify payroll calculation and configuration elements. • PSOPRCLS – Provides details on permissions linked to user profiles. Information from this table will identify users who have the relevant permission lists assigned directly to their user profiles. 2. In addition to the customised permission lists and roles identified in (1) above, access to standard PeopleSoft roles and permission lists should also be reviewed for usage as these default security items have powerful access and will allow for access to modify payroll calculation rules. Access to these roles and permission lists should be restricted as the norm. Default roles • PeopleSoft Administrator • PeopleTools • GP Administrator • Payroll Administrator • Payroll Interface Admin Permissions Lists HCCPSS1035: Pay-Employee PSADMIN: PeopleSoft Administrator HCCPGP1: Global Payroll HCCPPI1000: Payroll Interface HCCPPPS1000: Payroll Process Integration 3. Access to the following employee pay tables should be appropriately restricted: • PS_EARNINGS_TBL – Contains the positive payments made to employees driven by the compensation rate/salary, frequency, and so on. • PS_ADDL_PAY_DATA – Contains additional payroll information. • PS_GARN_SPEC – Contains information regarding deductions being made to a third party.

IMPORTANT UPDATE

R405: Payroll calculation is inaccurate or incomplete	
	• PS_JOB – Contains all the current and historical data about an employee's job such as status, salary/compensation, position, payroll settings, benefits status. • PS_GEN_DED_TBL – Contains information about deductions from earnings (that is, type, before or after tax, priority and schedule). Review changes made to the tables above via the PER029 Database Audit Report (Path – Workforce Administration, Workforce Reports, Database Audit) to check that changes are made by approved personnel and changes made are duly authorised. **M60:** *Review payroll control reports and variance reports.* Useful reports to review prior to finalisation of the payroll include: • Payroll Exception Reports are effective where there is little variation between pay periods. Approved documentation such as leave forms, new engagements, terminations, change in pay rate, and change in deductions should be available to justify the period variation; • Payroll Budget to Variance Reports are effective in identifying significant differences; and • Employee Changes Reports highlight new employees, terminated employees and transfers to ensure only current and valid employees are included in the pay run. Once the reviewer is satisfied with the payroll calculation, a final payroll report should be produced and a copy filed. Reports: • PAY035 report identifies any records that could cause errors during Pay Calculation. • PAY034 report indicates all errors that occurred when verifying the integrity of the payroll run prior to creating the paysheets. • PAY011 provides all Payroll Error Messages for Employees.

IMPORTANT UPDATE

R406: Statutory obligations for payment of taxation are breached	
Risk type	
Consequence	ATO requirements including PAYG and FBT payment requirements, are breached through failure to retain adequate records or report on and remit tax by specified deadlines, potentially resulting in penalties or reputational consequences.
Better practice	**S23:** *Restricted access to establish and amend taxation reference tables.* The ability to upload and amend tax tables within the HRMIS should be restricted and changes to reference data should be approved prior to the change being implemented. 1. Access to maintain tax table configuration is controlled through appropriate permission lists to the following path: (Path – Global Payroll, Payee Data, Taxes, Maintain Tax Data AUS) and should be appropriately restricted. 2. Review access to permissions lists and roles that have access to the path above. This can be done by reviewing information extracted from the following tables: • PSAUTHITEM – Provides details on permission lists that have been configured/enabled. Work with the PeopleSoft Administrator to determine the permission lists that have been customised which provide access to maintain tax data information. • PSROLECLASS – Provides details on permissions that are linked to roles. Information from this table will enable the determination of the roles that have the permission lists identified above which will help in determining users with such access. • PSROLEUSER – Provides details on roles linked to user profiles. Information from this table will identify users with access to modify payroll calculation and configuration elements. • PSOPRCLS – Provides details on permissions linked to user profiles. Information from this table will identify users who have the relevant permission lists assigned directly to their user profiles. **M61:** *Review and approval of Fringe Benefits Tax return by appropriate authority.* The amount of FBT payable is self-assessed by the entity. Prior to lodgement of the annual FBT return, detailed review should be undertaken by an appropriate person to determine whether: • Confirmation that a fringe benefit which has been provided is accurate; and • Where a fringe benefit has been provided, the applicable rates and thresholds have been accurately applied in the calculation outlined within the return.

IMPORTANT UPDATE

<table>
<tr><th colspan="2">R407: Breach of legislative requirements relating to superannuation</th></tr>
<tr><td>Risk type</td><td></td></tr>
<tr><td>Consequence</td><td>Insufficient superannuation is paid, or payment is not made prior to the quarterly cut-off date.

ATO guidance is contravened due to failure to retain adequate documentation in support of super contributions.</td></tr>
<tr><td>Better practice</td><td>S24: Configure automated calculation of superannuation payable.

Flagging employees as eligible or ineligible for super contributions and setting the percentage of super payable should enable the super amount payable per period to be automatically calculated by referencing the payroll calculations (for salaries and wages paid) and relevant master data, such as salary sacrifice amounts and additional employee contributions.

The following superannuation base elements should be appropriately configured:
<table>
<tr><th>Deduction</th><th>Field</th><th>Rationale</th></tr>
<tr><td>Mandatory Deduction (SGC_MAN)</td><td>AUS VR SGCMAN PCT</td><td>The Superannuation Guarantee (SG) contribution mandated by Australian legislation</td></tr>
<tr><td>Employer Additional Super (ER ADDLSPR)</td><td>SUP VR ERADDL PCT</td><td>The super contribution that the Entity is paying in addition to the 9 per cent mandated by legislation</td></tr>
</table>
Furthermore, there are other deduction elements to incorporate additional salary sacrifice deductions and/or employer matching deductions (Path – Set Up HRMS, Product Related, Global Payroll, System Settings, Element Types). The system then utilises the deduction values configured to undertake standard calculation rules which are based either on the percentage values defined or on predefined deduction value amounts. Note that PeopleSoft can perform deductions in both forms and this is likely to be customised based on the organisational requirements.</td></tr>
</table>

20 In computer programming, a schema refers to the organisation or structure of a database and generally defines the structure and content for each data element within the database structure.

IMPORTANT UPDATE

R408: Salary sacrifice arrangements are not appropriately managed	
Risk type	
Consequence	Salary sacrifice arrangements are not clearly documented and the components are not captured in the HRMIS, leading to inaccurate taxation calculations, payments, and disbursements. Non-allowable items are included as part of a salary sacrifice arrangement. This may lead to inaccurate fringe benefits and PAYG tax calculations.
Better practice	**S25:** *Salary sacrifice details are appropriately established in the HRMIS.* The ability to establish and amend salary sacrifice details in the HRMIS should be restricted to appropriate roles within the entity, having regard to enforcing effective segregation of duty controls. 1. PeopleSoft provides for preconfigured system functionality to review Salary Packaging information and current expenditure against budget (Path – Global Payroll, Absence and Payroll Processing, Review Absence/Payroll Info, Salary Package Summary AUS, Period Summary). 2. Review access to permissions lists and roles that have access to modify salary sacrifice/ salary packaging elements. This can be done by reviewing information extracted from the following tables: • PSAUTHITEM – Provides details on permission lists that have been configured/enabled. Work with the PeopleSoft Administrator to determine the permission lists that have been customised which provide access to modify payroll calculation rules. • PSROLECLASS – Provides details on permissions that are linked to roles. Information from this table will enable the determination of the roles that have the permission lists identified above which will help in determining users with such access. • PSROLEUSER – Provides details on roles linked to user profiles. Information from this table will identify users with the relevant access. • PSOPRCLS – Provides details on permissions linked to user profiles. Information from this table will identify users who have the relevant permission lists assigned directly to their user profiles. 3. In addition to the customised permission lists and roles identified in (2) above, access to standard PeopleSoft roles and permission lists should also be reviewed for usage as these default security items have powerful access and will allow for access to review salary packaging information. Access to these roles and permission lists should be restricted as the norm. Default roles • PeopleSoft Administrator • PeopleTools • Salary Packaging Admin AUS Permissions Lists HCCPHR4600: Admin Salary Packaging PSADMIN: PeopleSoft Administrator

IMPORTANT UPDATE

R408: Salary sacrifice arrangements are not appropriately managed	
	M62: *Review and monitor changes to key salary sacrifice information.* Set-up of the salary package elements and rules should be independently reviewed to ensure the following: • Configuration accurately reflects the documented salary sacrifice agreement; • The salary/wage component has been accurately captured to enable accurate PAYG withholding; • Sacrifices which constitute fringe benefits have been accurately classified and captured to enable accurate Fringe Benefits Tax self-assessment; • Sacrificed superannuation is set up as an employer contribution (to be subject to taxes associated with this type of contribution) effective 1 July 2009; and • Salary package elements outside the policy framework are not included as part of the arrangement.

R409: Methodology for performance payment is not established	
Risk type	
Consequence	Unauthorised or inaccurate bonus payments may be disbursed to employees. Bonuses may not be adequately accounted for throughout the period.
Better practice	**S26:** *Utilise system functionality to accrue for and calculate bonus payments.* Where bonus payments are based on a percentage of employee base salary or can be calculated using data established in the system, the automated accrual and payment calculation should be utilised to reduce the risk of inaccurate accrual and calculation. Where automatically calculated, the system output should be independently reviewed by an authorised HR representative for accuracy. Review bonus elements that have been configured (Path – *Set Up HRMS, Product Related, Global Payroll, System Settings, Element Types*). Review current values to date with the HR administrator to determine appropriateness of value (Path – *Set Up HRMS, Product Related, Base Benefits, Plan Reports, Leave Plan-Accrual and Bonus*).

IMPORTANT UPDATE

R410: Employee benefits are not managed or administered in accordance with employee agreements	
Risk type	
Consequence	Employees may receive benefits to which they are not entitled, potentially resulting in financial loss to the entity. Entity may breach terms of enterprise agreements through poor management of employee benefits process.
Better practice	**S27:** *Correctly establish and manage employee benefits.* Eligibility for employee benefits should be established by pay structure/employee role/employee type. When adding a participant, the system should be configured automatically to reference the position (if eligibility is based on level in the organisation) and should prevent participation of ineligible employees or employee classifications. If eligibility is based on information contained in master data (for example, years of service), master data should be automatically referenced to block participation of ineligible employees. System functionality enables the configuration of benefit plans and enables subsequent implementation and monitoring (Path – Set Up HRMS, Product Related, Base Benefits, Program Structure, and Benefit Program Table). Key configurable items are: • **Event Rules** – defines rules which determine eligibility based on an event which has occurred; for example, promotion, change in job grade (Path – Set Up HRMS, Product Related, Automated Benefits, Eligibility and Event Rules, Event Rules Table). • **Eligibility Rules** – defines eligibility for benefits based on a personnel, job and geographical/ location criteria as well as rules to ensure singularity of benefits per employee (Path – Set Up HRMS, Product Related, Automated Benefits, Eligibility and Event Rules, Eligibility Rules Table). • **Cost** – benefits costs which include rates and calculation rules (Path – Set Up HRMS, Product Related, Base Benefits, Program Structure, and Benefit Program Table). **S28:** *Restricted access to establish benefit plans.* Access to establish benefit plans, enrol employees, create employee specific information associated with the plan and amend plan or employee information should be restricted to appropriately authorised personnel. 1. Review access to permissions lists and roles that have access to maintain benefits plans. This can be done by reviewing information extracted from the following tables: • PSAUTHITEM – Provides details on permission lists that have been configured/enabled. Work with the PeopleSoft Administrator to determine the permission lists that have been customised which provide access to maintain benefits plans. • PSROLECLASS – Provides details on permissions that are linked to roles. Information from this table will enable the determination of the roles that have the permission lists identified above, which will help in determining users with such access. • PSROLEUSER – Provides details on roles linked to user profiles. Information from this table willidentify users with the relevant access. • PSOPRCLS – Provides details on permissions linked to user profiles. Information from this table will identify users who have the relevant permission lists assigned directly to their user profiles.

IMPORTANT UPDATE

<table>
<tr><th colspan="2">R410: Employee benefits are not managed or administered in accordance with employee agreements</th></tr>
<tr><td></td><td>2. In addition to the customised permission lists and roles identified in (1) above, access to standard PeopleSoft roles and permission lists should also be reviewed for usage as these default security items have powerful access and will allow for access to establish benefit plans. Access to these roles and permission lists should be restricted as the norm.

Default roles

• PeopleSoft Administrator
• PeopleTools
• Benefits Administrator

Permissions Lists

HCCPBN1000: Benefits
HCCPPY2000: Retro Benefits/Deductions
HCCPSS1020: Benefits-Employee</td></tr>
</table>

6.4 PeopleSoft controls for system maintenance and integration

The control considerations in managing and maintaining PeopleSoft should be consistent with those for other key business systems of the agency. Specific control elements which should be given additional consideration would include change management and interface management. Owing to the complexity of and potential confidentiality considerations arising from changes made within the HRMIS context, additional consideration should be given to checking that changes made to employee data and payroll configuration values are approved changes. Interface management controls over internal and external system interfaces between the HRMIS should have appropriate controls to safeguard the sensitive information from a confidentiality and completeness perspective.

Implementation of payroll configuration

Within a PeopleSoft environment, establishment and configuration of payroll elements and rules in the Human Resources and Global Payroll Tables and the interface with payroll master data elements, is the necessary step to enable an accurate and automated calculation. Further configuration of elements and rules will enable payroll processing in line with an entity's requirements, while specialised elements and rules can assist with meeting legislative superannuation and payroll taxation requirements.

In PeopleSoft, the relationship between payroll configuration and other system elements (master data tables, workforce configuration values, and transactional data) enables complete and timely payroll processing.

IMPORTANT UPDATE

Key control objectives

Control objective	Risks mitigated
Payroll information is completely and accurately posted to the General Ledger via the payroll journal.	**R501:** Payroll system does not reconcile to the General Ledger.
Information regarding superannuation contributions is submitted to superannuation funds (such as ComSuper) via an automated interface, ensuring complete and accurate transfer of data.	**R502:** Incomplete or inaccurate submission of superannuation data.
The rate at which leave accrues and leave types to which employees are entitled is accurately established.	**R503:** Leave accrual rates are established inaccurately.
Fields requiring translation into a foreign currency correctly reference accurate foreign exchange rates within the HRMIS to enable accurate calculations.	**R504:** Employee wages paid in foreign currency are calculated incorrectly.
The organisational chart within the application is continuously maintained to accurately reflect vacant and filled positions within the entity, assisting with position management and recruiting efforts.	**R505:** The HR system organisational chart does not accurately reflect current employees and their position.
Payroll schemas and business processing rules are comprehensively and accurately established to enable a stable payroll calculation requiring minimal manual intervention, and are protected from unauthorised modification.	**R506:** Payroll schemas established or modified inaccurately or without authorisation.
Risks to business systems are generally reduced when available patches are installed in a timely manner after being tested for reliability and usability.	**R507:** Application is vulnerable to security or availability threats.

IMPORTANT UPDATE

Risks and controls

R501: Payroll system does not reconcile to the General Ledger	
Risk type	
Consequence	The payroll system should reconcile to the General Ledger to ensure integrity of the financial statements. If not reconciled, or reconciled incorrectly, there is an increased risk of material misstatement in the financial statements.
Better practice	**S29:** *Utilise auto-posting functionality.* Where auto-posting functionality is available within the application, it should be utilised to update the General Ledger. Appropriate configuration between the systems is required, and this should be manually triggered so that only final approved payroll results are updated to the General Ledger. GL interface settings in place can be reviewed (Path – Set Up HRMS, Product Related, Global Payroll, Integration, Journal Type AUS). This path specifies the journal types configured for the GL interface. While this is not specifically an automated reconciliation process, these settings provide an overview of the manner in which the GL interface has been configured. **M63:** *Review of payroll posting results.* A review of payroll results that have not posted to the General Ledger should be performed at each pay cycle. If payroll transactions are manually posted (or a file manually uploaded into the General Ledger), a reconciliation should be performed and payroll that is not posted should be actioned.

R501: Payroll system does not reconcile to the General Ledger	
Risk type	
Consequence	The payroll system should reconcile to the General Ledger to ensure integrity of the financial statements. If not reconciled, or reconciled incorrectly, there is an increased risk of material misstatement in the financial statements.
Better practice	**S29:** *Utilise auto-posting functionality.* Where auto-posting functionality is available within the application, it should be utilised to update the General Ledger. Appropriate configuration between the systems is required, and this should be manually triggered so that only final approved payroll results are updated to the General Ledger. Maintain controls at the interface (as an example) to assist in accurate remittance of amounts to the superannuation fund. **M63:** *Review of payroll posting results.* A review of payroll results that have not posted to the General Ledger should be performed at each pay cycle. If payroll transactions are manually posted (or a file manually uploaded into the General Ledger), a reconciliation should be performed and payroll that is not posted should be actioned.

IMPORTANT UPDATE

R502: Incomplete or inaccurate submission of superannuation data	
Risk type	
Consequence	Information submitted to the superannuation fund is incomplete or inaccurate, potentially leading to penalty payments or incorrect reporting of superannuation payments.
Better practice	**S30:** *Superannuation data is provided in the required format and in the required timeframes.* Superannuation data should be provided in the required format and in the required timeframes as defined by the relevant recipient. Where available, the entity should generate such reports and data from the payroll system data. Maintain controls at the interface (ComSuper as an example) to assist in accurate remittance of amounts to the superannuation fund. **S31:** *Changes to superannuation interfaces and data file formats are managed using entity IT change management controls.* Changes and upgrades to the HRMIS should not inadvertently modify customised interfaces or data files. This control is not configurable in PeopleSoft.

R503: Leave accrual rates are established inaccurately	
Risk type	
Consequence	Inaccuracies in leave accruals reduce the accuracy and reliability of the payroll calculation and associated financial reports.
Better practice	**S32:** *Manage leave accrual rules.* Leave accrual rules are used to calculate employee leave accruals. The leave accrual rules should be consistent with employee conditions for employment (and/or employee agreement) and linked within the application to employee entitlement information. In PeopleSoft, absence rules define the parameters for enrolling and terminating an employee for a specified leave class. Depending on organisational requirements, there could be default enrolments for Annual and Sick leave and other types of customised leave types (Home leave as an example) that are configured. Absence rules typically address the following criteria: **S33:** *Configuration of maximum values for leave accruals.* If employee conditions of employment specify a maximum amount of leave which can be accrued or carried forward, maximum values should be configured for each type of leave accrual. If the maximum leave accrual amount is reached, an error message should be reported and the system designed to stop accruing further leave. As per S32. Review absence rules that have been set up (Path – Set Up HRMS, Product Related, GlobalPayroll & Absence Mgmt, System Settings, Element Type). **M64:** *Regular review of employees' leave accruals should be performed.* A manual review of employee's leave accruals should be performed by managers to assess for reasonableness against known periods of leave taken by employees. A further review should be performed by HR to identify any excessive or negative balances. Report: GPAUAM02 – this report displays leave accrual information by leave class and employee. It includes information such as year eligibility hours, carryover hours earned year-to-date, hours taken year-to-date, and remaining leave balance.

IMPORTANT UPDATE

R504: Employee wages paid in foreign currency are calculated incorrectly	
Risk type	
Consequence	Use of inaccurate foreign exchange rates for currency translation purposes will result in inaccurate calculation of payroll.
Better practice	**S34:** *Establish automated updates for foreign exchange rates.* An automated update of foreign exchange rates should be established with an authorised source and the entity application to ensure rates applied are up to date and accurate. Controls will be dependent on the manner in which the entity has configured the update of exchange rate information. The actual rates configured and their rate values can be reviewed via system reports. Currency Code Table report (PER713) outlines information on the various currencies configured in the system and Currency Rate Table report (PER714) outlines the exchange rates utilised for the various currencies.

R505: The HR system organisational chart does not accurately reflect current employees and their positions	
Risk type	
Consequence	Incomplete organisation chart may impair the accuracy of workflows associated with self-service functionality, and user access privileges. Other impairments include headcount errors and incorrect workforce planning decisions.
Better practice	**S35:** *Restricted access to update organisational chart.* Access to update the organisational chart should be restricted to appropriate personnel. Amendments should only be processed based on appropriately approved documentation (for example, authority to create a new position). Access to make organisation position changes and review are via Path – Set Up HRMS, Product Related, Organizational Development, Position Management, Maintain Positions/Budgets, Add/Update Position Info, Budget and Incumbents. Review access to this page by undertaking the following: 1. Review access to permissions lists and roles that have access to make organisational changes. This can be done by reviewing information extracted from the following tables: • PSAUTHITEM – Provides details on permission lists that have been configured/enabled. Work with the PeopleSoft Administrator to determine the permission lists that have been customised which provide access. • PSROLECLASS – Provides details on permissions that are linked to roles. Information from this table will enable the determination of the roles that have the permission lists identified above which will help in determining users with such access. • PSROLEUSER – Provides details on roles linked to user profiles. Information from this table will identify users with the relevant access. • PSOPRCLS – Provides details on permissions linked to user profiles. Information from this table will identify users who have the relevant permission lists assigned directly to their user profiles.

IMPORTANT UPDATE

R505: The HR system organisational chart does not accurately reflect current employees and their positions	
	2. In addition to the customised permission lists and roles identified in (1) above, access to standard PeopleSoft roles and permission lists should also be reviewed for usage as these default security items have powerful access and will allow for access to update the organisational structure. Access to these roles and permission lists should be restricted as the norm. Default roles • PeopleSoft Administrator • PeopleTools Permissions Lists HCCPHR3100: Maintain Positions HCCPHR3310 Data: Job Data **S36:** *Ability to display temporary assignments.* Functionality enabling the organisational chart to display temporary assignments should be utilised to enable tracking of higher duties assignments. Review temporary assignments without end dates to determine appropriateness of assignment (Path-Workforce Administration, Job Information, Temporary Assignments, Temp Assignment without End Date). Useful reports include Temp Assignment without End Date report (TAS001) which lists employees currently on temporary assignment where end dates have not been defined and Temp Assignment due to Complete report (TAS002) which lists employees due to complete temporary assignments within specified date ranges. **S37:** *Organisational chart designed to reflect the hierarchy.* The organisational chart should be designed to reflect the hierarchy for each department or organisational unit. Refer to S35.

IMPORTANT UPDATE

R506: Payroll schemas established or modified inaccurately or without authorisation	
Risk type	
Consequence	Payroll accuracy is impacted as a result of errors caused by the incorrect set-up of payroll schemas or rules that cause the schemas to execute calculations inaccurately.
Better practice	**S38:** *Access to establish or modify payroll schemas or elements and rules is restricted.* Access to set up or modify payroll schemas or elements and rules should be restricted to appropriate personnel. Access to payroll calculation elements (Path *Set Up HRMS, Product Related, Global Payroll, System Settings, Element Types*) should be controlled and restricted via appropriate permission lists and roles. Review access to this page by undertaking the following: 1. Review access to permissions lists and roles that have access to make organisational changes. This can be done by reviewing information extracted from the following tables: • PSAUTHITEM – Provides details on permission lists that have been configured /enabled. Work with the PeopleSoft Administrator to determine the permission lists that have been customised which provide access. • PSROLECLASS – Provides details on permissions that are linked to roles. Information from this table will enable the determination of the roles that have the permission lists identified above which will help in determining users with such access. • PSROLEUSER – Provides details on roles linked to user profiles. Information from this table will identify users with the relevant access. • PSOPRCLS – Provides details on permissions linked to user profiles. Information from this table will identify users who have the relevant permission lists assigned directly to their user profiles. 2. In addition to the above, assess whether access to role and permission lists, including default roles and permissions lists that enable access, is appropriately restricted: Default Roles • PeopleSoft Administrator • PeopleTools • GP Administrator • Payroll Administrator • Payroll Interface Admin Permission Lists HCCPSS1035: Pay-Employee PSADMIN: PeopleSoft Administrator HCCPGP1: Global Payroll HCCPPI1000: Payroll Interface HCCPPPS1000: Payroll Process Integration

IMPORTANT UPDATE

R506: Payroll schemas established or modified inaccurately or without authorisation	
	3. Access to the following employee master record tables should be appropriately restricted: • PS_EARNINGS_TBL – Contains the positive payments made to employees driven by the compensation rate/salary, frequency, and so on. • PS_ADDL_PAY_DATA – Contains additional payroll information. • PS_GARN_SPEC – Contains information regarding deductions being made to a third party. • PS_JOB – Contains all the current and historical data about an employee's job such as status, salary/compensation, position, payroll settings, and benefits status. • PS_GEN_DED_TBL – Contains information about deductions from earnings (that is, type, before or after tax, priority, and schedule). Review changes made to critical tables via the PER029 Database Audit Report (Path – *Workforce Administration, Workforce Reports, Database Audit*) to determine if changes made have been undertaken by authorised personnel.

R507: Application is vulnerable to security and availability threats	
Risk type	
Consequence	A software update is not installed in a timely manner or not installed completely and accurately, making the application vulnerable to security breaches and threatening the availability of the application.
Better practice	**S39:** *Automatic notification of available software updates.* Automatic notification should be configured to alert the system administrator whenever a software update is available. Automatic notification is available through a prescribed process via the application account management process (Oracle) which allows for email updates to be received by nominated personnel within the organisation when new patches are released. This process is performed outside of PeopleSoft. **M65:** *Timely installation of approved software updates.* All software updates should be tested in a controlled environment (replicating the production environment) before being released into production.

IMPORTANT UPDATE

6.5 Useful reports for PeopleSoft Human Capital Management

The *PeopleSoft Human Capital Management module* provides standard reporting functionality. The table below provides a list of specific reports to the HR functions that are useful tools for both management decision making and internal controls. The list does not include customised reports which will be different for each agency.

Code	Name	Description
HR and payroll data management		
PAY711	Pay Group Report	Prints each pay group and its effective date along with the processing characteristics that apply to that group. This report will enable the user to review the appropriateness of the various paygroups set up as part payroll master data.
PER701	Department Table ID	Overview of all configured departments in master data. This report will enable the user to review the appropriateness of the departmental structures set up as part of payroll master data.
PER702	Installation Table Report	Overview of default configuration values. This report provides an overview of default configurable items such as minimum/maximum working hours and default agency information.
PER709	Job Code Table Report	Prints a list of all job codes and the date on which they become effective, which will assist with determining the appropriateness of master data set up.
PER705	Location Table Report	Overview of all configured locations in master data. This report will enable the user to review the appropriateness of the business/organisational locations set up as part of employee master data.
PER707	Company Table Report	Overview of all configured companies (company code) in master data. This report will enable the user to review the appropriateness of the companies set up as part of employee master data.
PER710	Action Code Report	This report will enable the user to review the various action codes (for master data change/movement) that have been configured, which will be useful in reviewing the appropriateness of master data changes.
Workforce management		
Employee commencements		
PER029	Database Audit	Monitors changes, additions and deletions made to sensitive fields. This is a useful report to review changes made to employee data and to check that changes are undertaken in an authorised manner.
PER506	Department Security Tree	Lists discrepancies between the data entered in the Department Tree and the departments added to the current security tree. This report will assist in reviewing departmental security configuration.
PER015	Personnel History Report	Overview report that provides the following information on employees: employee name, original hire date, total years of service, employee status, job code and title, salary grade, and supervisor name.
PERZ021	Pending Actions Report	Report provides list of employees with job actions specified for the future. Useful report to review the completeness of employee on-boarding and termination process.

IMPORTANT UPDATE

Code	Name	Description
APP003	Requisition Status	For each job requisition, the report lists job information, requisition status, recruiter, the number of applicants, and expenses information. This report will assist in determining whether the employee on-boarding process was undertaken in an appropriate manner.
APP005	Candidate Listing	Combines job requisition information with a list of candidates being interviewed for the position. It groups requisitions by Department ID. For each candidate interviewed, the report displays the following: • employee ID; • name, status in the interview process (active, inactive, hired, withdrawn); • last interview; • step completed; and • any offers made.
APP006	Requisition Cost Analysis	Provides a breakdown of expense types and amounts for each job requisition. A useful report to review to determine costs incurred in on-boarding employees.
Position management		
PER058	Employee Listing	Lists all employees and/or non-employees with multiple primary jobs, terminated or with no primary jobs. An exception report to review employees with no primary jobs which can then be utilised as a follow-up with management on rationale/further actions to be undertaken.
PER081	Employee Listing	Provides a list of all employees as at a selected date (by employee name, ID and Department).
PER007	Temporary Employee Listing	This report lists all temporary employees as at a selected date.
POS002	Active/Inactive Positions	Lists the current position related data for active positions and inactive positions.
POS003	Employment History by Position	Provides incumbent history information on all filled positions.
POS001	Listing of Positions	An overview of all positions defined within the current organisational structure.
POS008	Position Exception report	Position exception/override exception reporting. A useful report to review for position management exceptions and subsequently check that such exceptions have been appropriately approved.
TC003	Employee Compensation Report	Detailed information about each compensation type for each individual within a group specified.
HEP001	Missing Documents	Report to review the performance management process. Lists missing documents for a group of employees (Group ID) and a given document type and date range.
HEP002	Late Documents	Report to review the performance management process. Lists manager documents for which the due date has passed.
Employee exits and terminations		
CNT001	Contract Information	Lists the contract history for a selected employee or all employees. Exception report to review contract information for specific employees.
PER010	Employee Turnover Analysis	Assists with analysis of employee turnover and can be generated by department/cost centre.

Code	Name	Description
POS002	Active/Inactive Positions	Lists the current position-related data for active positions and inactive positions.
POS007	Listing of all Current Vacant positions	Listing of all current vacant positions.
PER019	Terminations Analysis	Terminations analysis by reason codes, dates and so on. A useful report to assist in reviewing termination payments.
TAS001	Temp Assignment without End Date	Lists all employees on temporary assignments without a specified end date.
TAS002	Temp Assignment due to Complete report	This report lists all employees who are due to complete temporary assignments within a specified data range.
Time reporting		
TL001	Payable Status Report	Provides an overview of employee time incurred by date.
TL004	Schedule Hours Report	This report outlines scheduled hours per employee.
Payroll processing and administration		
PAY711	Pay Group Report	Shows each pay group and the processing characteristics that apply to that group. This report enables the user to review the appropriateness of the payroll master data set up.
PER029	Database Audit	Monitors changes, additions, or deletions made to sensitive fields such as salary amounts. This report provides an audit trail of changes undertaken and allows the user to review whether these changes were duly authorised.
PER013	Compensation Rate Change	Lists employees who have had compensation rate changes within a selected time period. The report provides an audit trail of changes made.
PER713	Currency Code Table Report	Provides a listing of all currency codes that have been configured.
PER714	Currency Rate Table Report	Provides the exchange rates that have been captured for the various currency codes configured.
VC009	Compensation Approval Report	The report provides information about payroll compensation with approver information by payout period for specific periods.
VC010	Variance Report	Review variance between target and actual payouts. This report will enable the user to monitor actual vs. estimated payroll costs.
BAS001	Eligible Participants	Lists, by schedule and benefit program, employees that are eligible to participate in company benefit programs with details on plan and option eligibility. Overview report that allows the user to review benefits offered and eligible participants.
BAS003	Invalid Benefit Elections	Lists, by schedule and event, participants and their dependents, showing any errors such as coverage over the maximum or under the minimum, invalid choices, failure to meet eligibility requirements, and so on. An exception report that can be reviewed and subsequently followed up for rationale/management action.
BAS010	Ineligible Participants	Lists all participants ineligible for any benefit program and their eligibility parameters, such as birth-date and status. Exception reporting which allows for subsequent follow-up.

IMPORTANT UPDATE

Code	Name	Description
BAS702A	Benefit Program/ Plan/Options	For a specified benefit program, prints program-level information (effective date and status, program type, age criteria), along with the plan and option-level structure (event rules, eligibility rules, coverage levels and deduction codes). Report to review master data elements in configuring benefits.
BAS703A	Eligibility Rules	For each plan type in a benefit program, prints the rules for minimum standard hours, maximum standard hours, minimum service, maximum service, minimum age, maximum age, service and 'age as of' information, employee class, employee status, employee type, full/part, regular/temp, officer code, union code, company, location, state and eligibility configuration. Report allows the user to review the configurable elements for benefits and determine the appropriateness of the values configured.
BAS003	BenAdmin Preparation and Election Errors	Audit trail checks for changes made to correct errors or to perform updates. The report allows the user to review changes made and determine the appropriateness of changes.
PKG006	Salary Packaging FBT Reconciliation – Administer Salary Packaging	In the FBT Reconciliation Report, all FBT categories are identified based on the component types defined on the Package Component table. For each component type, or FBT category, employees who have received this benefit in the FBT year are outlined. A useful report to consider in reviewing the salary packaging process for the agency.
PKG004	Package Model	An overview report that provides salary package information by employee, annual package and period amounts, and deductions.
GPAUPSO1	Payment Summary	Reporting on year end payee requirements in line with ATO requirements. A report to review the appropriateness of tax amounts deducted from employees.
GPAUPY21	Payment Summary Exceptions	Identifies discrepancies between the year-to-date amounts and actual results per period to avoid problems with payment summaries at year end. Exception report to enable follow up on rationale/follow-up actions required.
PAY034	PreSheet Audit Report	Indicates all errors that occurred when verifying the integrity of the payroll run.
PAY035	PreCalculation Report	Identifies potential errors due to data integrity issues prior to payroll calculation being run.
PAY011	Payroll Error Message for Employees	Outlines all the error messages encountered in performing the payroll calculation.
GPAUAM02	Leave Accruals	Provides information on leave accruals by eligible hours, hours taken and balance.

IMPORTANT UPDATE

7. SAP – Human Capital Management

The chapter provides detail on the risks and controls by HR function as managed by the SAP human capital management.

7.1 SAP controls for HR and payroll data management

The employee master file is the central element of all system control within SAP. Employee information is stored in different infotype records and is drawn upon by nearly every activity in the Payroll process including time entry, payroll processing and benefits administration. Information maintained in the employee master record is sensitive and subject to privacy and legislative requirements and therefore should be adequately controlled. This information includes the employees name, address, contact details and tax file number.

Further information on the functionality, risks and controls of the SAP module is available in the *SAP ECC 6.0 Security and Control Better Practice Guide*.[18]

Key control objectives

Control objective	Risks mitigated
HR and payroll data is appropriately maintained to provide accurate and complete employee information and payroll transactions	**R201:** HR master data is inaccurate. **R202:** HR master data is not secure.

Risks and Controls

R201: HR master data is inaccurate	
Risk type	
Consequence	Employee details may be incorrectly entered or maintained, which may result in duplicate payments, errors with superannuation contributions or employee deductions, or unapproved changes to the allocation of roles and delegations
Better practice	**S01:** *Define key data entry fields.* Key data fields should be defined in the system to confirm that information necessary to the completion of master data is entered. Key data entry fields should be defined as 'required entry' in the system to ensure that all information necessary to the completion of HR master data is entered. Field settings are able to be controlled for both screen headers and the detailed section of the screen. The standard system settings are defaulted but should be reviewed to ensure that appropriate settings are defined for each entity. The infotype audit report (RPUAUD00) is a critical control report within SAP payroll. It is configurable and can be used to review changes to key payroll records. This report can be used to identify ghost or duplicate employee or employee integrity issues created within the payroll system.

18 The *SAP ECC 6.0 Security and Control Better Practice Guide* released in June 2009 is available for download at the ANAO website, or a printed version is available by contacting the ANAO on 02 6203 7300 or via email on: publications.team@anao.gov.au.

IMPORTANT UPDATE

R201: HR master data is inaccurate	
	S02: *Restricting user access to view, establish and update master data.* Access to view, establish and update master data should be restricted to appropriately authorised users. Users with the ability to view master data should also be appropriately restricted to reduce the likelihood of inappropriate viewing or distribution of data. Access to employee maintenance transactions like PA30 must be restricted to key payroll staff. Access to maintain incompatible infotypes like basic pay 0008 and bank details 0009 should be restricted. (Refer to table 1 for further detail. Authorisation object P_PERNR should be used to restrict the ability of payroll staff to maintain their own payroll records. Access to employee maintenance using SAP transactions like PA30 – Maintain HR Master Data, must be segregated from the ability to maintain payroll configuration through SAP transactions like PE01 – HR: Maintain Payroll Schemas, PE02 – HR: Maintain Calculation Rules or PE01N – HR: Maintain Payroll Schemas. Controls over ensuring appropriate access to sensitive employee master records is reflected in control S04. Access to maintain incompatible infotypes like basic pay 0008 and bank details 0009 should be restricted. (Refer to table 10 for further detail). **S03:** *Validation checks on certain fields warn the user that the information is duplicated in another employee record.* Validation checks should be configured to decrease the likelihood of inaccurate information being entered (for example, tax file number cannot be duplicated in another employee record). SAP does not provide a duplicate employee check similar to what is provided in vendor maintenance in the Purchase & Payables process. **M50:** *Establishment and amendment of master data occurs only when supported by appropriately approved documentation.* All master data established and all amendments processed to master data should be supported by appropriate documentation (approved by an appropriate authority where relevant). Report: The infotype audit report (RPUAUD00) should be used to assess whether changes to sensitive and critical master records are appropriate and have been adequately authorised.

IMPORTANT UPDATE

R202: HR master data is not secure	
Risk type	
Consequence	Unauthorised users may have access to view and maintain sensitive HR and payroll data, which may compromise the confidentiality of personnel records and may also result in the processing of fraudulent payroll payments.
Better practice	**S04:** *Access to HR master data is appropriately configured and managed.* Implementing appropriate user access controls requires: • Identification and implementation of segregation of duty requirements in relation to validating updates/modification/deletion of master data within the HRMIS is complete and appropriately authorised; • Access to the application and to underlying data (such as the database) is assigned based on user profiles and/or roles; and • Employees should be limited in their ability to modify reference data items (salary, leave records and employment date) for their own records. With Web Client applications—like employee self-service (ESS)— the client may allow an employee to be able to modify their own data with the exception of high-risk data fields, including salary, hourly rate, additional pay, job grade. Access controls provide appropriate restrictions to user access to certain data types. Access should be controlled at three levels: • Restrict access to appropriate users (for example, HR personnel but in some situations access may be wider if ESS is implemented); • For each authorised user, restrict access to particular types of master data (for example, only some authorised users will have access to bank details); and • For each user and each type of data, specify whether access is 'view' or 'edit' access. **S02:** *Restricting user access to view, establish and update master data is also relevant.* **M51:** *Review of system configuration reports.* Generally system configuration change reports are available from the HRMIS and may be reviewed periodically to monitor changes to key controls or configuration settings. Such reports should be run periodically. Consideration should be given to ensuring that appropriate 'audit' tables and associated logs are also configured. Failure to configure such tables may mean that important information is not available for inclusion in monitoring reports. Reports: produced from either the SAP SUIM tool or through security products like SAP GRC should be regularly reviewed to determine whether access to sensitive HR master data is appropriately restricted. At a minimum access to transaction PA30 and PA40 and sensitive infotypes like PA0008 (Basic Pay) and PA0006 (Address details) should be reviewed.

IMPORTANT UPDATE

7.2 SAP controls for workforce management

Key control objectives

Control objective	Risks mitigated
Appropriate and accurate employee information is collected and maintained.	**R301:** Non-existent or duplicate employee is added to the payroll. **R302:** Termination payments and balances are inaccurately calculated. **R303:** Employee is not deactivated when employment is terminated.

Risks and Controls

R301: Non-existent or duplicate employee is added to the payroll	
Risk type	
Consequence	'Ghost' or duplicate employees on the payroll lead to overpayment or processing of fraudulent payments.
Better practice	**S05:** *Access to add an employee should be restricted to appropriate individuals and segregated from payroll maintenance.* Access to modify employee information should be restricted to decrease the likelihood of inappropriate or unapproved changes to employee information which may impact upon the accuracy and completeness of information maintained in the HRMIS. Additionally, restricting access in accordance with privacy principles reduces the risk of inappropriate disclosure of employee information. *Also refer to **S03:** Validation checks on key fields warn the user that the information is duplicated in another employee record.* When creating employee records it is important to use SAP to match codes to determine if the employee has already been created within the system. This check should be performed based on name and date of birth. In SAP, when the creation of a personnel number (PERNR) is attempted, SAP will check by default whether any existing PERNR exists that has the same name and date of birth. If a record exists, the system will produce a warning message (note that it is only a warning message, not an error message). The infotype audit report (RPUAUD00) is a critical control report within SAP payroll. It is configurable and can be used to review changes to key payroll records. This report can be used to identify ghost or duplicate employee or employee integrity issues created within the payroll system. Effective management of the organisation structure and chart reduces the risk of ghost employees. **M52:** *When adding a new employee, a listing of current employees should be reviewed to reduce the risk of duplicating the employee record.* A system report of all current employees should be generated prior to adding a new employee, and checked to confirm the employee does not already exist in the system.

IMPORTANT UPDATE

R301: Non-existent or duplicate employee is added to the payroll	
	A system report of all new employee additions should be generated monthly and an individual who is independent from the employee set-up process should check each addition against supporting paperwork (for example, approval to engage, employee information including bank account) to validate the set-up was authorised and has been completed accurately. Report: A system report of all current employees, report S_AHR_61016376 employee listing, should be generated prior to adding a new employee, and checked to ensure the employee does not already exist in the system.

R302: Termination payments and balances are inaccurately calculated	
Risk type	
Consequence	Termination payment is incorrect, resulting in incorrect salary and leave entitlements being paid or reported
Better practice	**S06:** *Application will warn user if termination date in the past is entered.* The system should be configured such that if a termination date in the past is entered, a warning message is generated to reduce the occurrence of backdating of terminations and to accurately process termination payments and calculations. SAP can be configured to provide a warning or error message where the termination date is entered in the past. Typically organisations using SAP will remove the user from their position in the organisation chart which automatically stops payment to the employee. **S07:** *Workflow operates to require independent approval verification of termination date entered.* Automated workflow approvals utilising organisation hierarchy positions delegations of authority should be utilised to approve terminations. The approver should verify the termination date of the employee prior to approving. SAP workflow can be used to enable automated approval of employee terminations. Workflows determine required approvals and subsequent work steps. **S08:** *Application automatically calculates payments based on master data, termination date entered, and leave entitlements.* Use of system functionality to calculate and report entitlements and balances is more accurate. The effectiveness of this control requires accurate data entry and maintenance of employee information and master data. The SAP termination program automatically calculates an employee's final payment based on employee pay and leave entitlements. The Termination Workbench computes the various types of payments – for example, gratuity, superannuation, leave encashment or any pending reimbursable allowances – due to, or payable by the employee at the date the termination is recorded. **M53:** *An independent authority checks the termination date per notification documentation to the date entered in the system.* On a monthly basis, a report of all terminations is generated and an individual who does not have access to terminate employees checks that all termination dates were accurately entered, with reference to termination documentation (for example, resignation letter). Report: On a monthly basis, the Termination Workbench, SAP transaction code PCOO_M40_TERM can be used to report on terminations.

IMPORTANT UPDATE

R303: Employee is not inactivated when employment is terminated	
Risk type	
Consequence	Employee record is not flagged as terminated which may result in subsequent payment to the employee. For agencies using 'single sign on' (which enables access to all applications without requiring separate passwords, by using credentials at the network sign-on level), failure to inactivate terminated employees may also fail to inactivate network access.
Better practice	**S09:** *Application automatically changes status of employee to 'terminated' as at termination date entered.* Systems are configured to automatically change the status of employees to 'terminated' as at the entered termination date. This is typically enabled through automated batch processing. SAP can be set to automatically change the status of employees to 'terminated' as at the entered termination date When the termination workbench is used, a batch session is run which records the employee as terminated using the actions infotype (0000). **S10:** *Application automatically disables terminated employee's access to systems based on termination date entered.* This control is possible where position-based security is utilised. Appropriate use of the termination date is important where single-sign access is granted based on a commencement or termination date. If position-based security is used, then removing a terminated employee from a position will automatically remove their access to the SAP system. Removing access in a user based security structure relies on SAP security administration staff manually removing the user's access. **S11:** *Application does not allow payment to be disbursed to employees with 'terminated' status.* Operation of this control typically does not require specific configuration within the system, as it is deemed 'standard' functionality. It may be possible in some circumstances to process ad-hoc payments to terminated employees using some applications. Automatic payments cannot be processed to a terminated employee. Off Cycle payments are typically used to pay employee ad hoc payments. **M54:** *Department/Cost Centre managers are periodically provided with a listing of employees for which they are responsible. This listing is checked to determine whether it contains any employees no longer working within the department.* System generated listings of current employees per department/area/cost centre should be provided to relevant managers to verify current employees. This check assists in detecting employees who have transferred or been terminated and information regarding the transfer or termination has not been recorded in the system. Reports: SL9C_94000095 – Headcount Changes; and S_ALR_87013611 – Cost Center Manager Review.

IMPORTANT UPDATE

7.3 SAP controls for payroll processing and administration

The ability to process payroll transactions—such as timesheet entry; and exception-based events, such as changes in pay rates—must be effectively controlled to enable accurate payroll processing. Key areas to consider include:

- SAP provides a central component (CATS) for the entry and approval of timesheets. The component provides the ability for workflow approvals of all time entered;
- Employee leave and other benefits are recorded as wage types within SAP; and
- Reviewing key exception-based reports including the RPCLJNU0 – Payroll journal and RPURECG0 – run to run reconciliation report is a critical control element used in SAP environments to identify exceptions in payroll processing.

Key control objectives

Control objective	Risks mitigated
Evidence of employee service and time is accurately recorded in the appropriate period.	**R401:** Inaccurate or incomplete entry of employee time data. **R402:** Unapproved leave or leave is taken outside of entitlements. **R403:** Established employee shifts are updated inaccurately. **R404:** Time recorded in prior periods is amended inaccurately or without appropriate authority.
Evidence of employee service and time is accurately recorded in the appropriate period.	**R405:** Payroll calculation is inaccurate or incomplete.
Evidence of employee service and time is accurately recorded in the appropriate period.	**R406:** Statutory obligations for payment of taxation are breached. **R407:** Breach of legislative requirements relating to superannuation. **R408:** Salary sacrifice arrangements are not appropriately managed.
Evidence of employee service and time is accurately recorded in the appropriate period.	**R409:** Methodology for bonus rewards is not established. **R410:** Employee benefits are not managed or administered in accordance with Workplace Agreements/employee contracts.

IMPORTANT UPDATE

Risks and controls

R401: Inaccurate or incomplete entry of employee time data	
Risk type	
Consequence	Time data entered does not accurately reflect time worked or does not include leave taken. Employee receives payment for hours or leave to which they are not entitled.
Better practice	**S12:** *Workflow approval of employee time.* Where workflow functionality is used, such as in self-service, the workflow should be configured so that submitted employee time is automatically routed through the workflow approval hierarchy for review by the employee's immediate supervisor or functional manager. The workflow should also be used to send rejected time allocations or leave requests to the employee via the system with the reason recorded. Workflow approvals for all timesheet entry can be established within each Timesheet/Employee Self Service profile. It is important to simplify the layout of the time sheet and the procedure for entering data. This means that even users with little or no experience of the SAP R/3 System can easily maintain data. **S13:** *System validation of data entered.* Validation checks should be configured to decrease the likelihood of inaccurate time being entered (for example, minimum/maximum number of working hours, checks against established time codes). The system may also be configured to provide default timesheets to employees with standard responsibilities and working hours. Timesheet/Employee Self Service profiles must be established to ensure timesheet validity. In the profiles, there are various settings that must be established including target hours, with total lines, with clock times and no deduction of breaks and so on. Error messages can also be defined in the profiles (for example, an employee already booked an absence on a particular day and again booked the absence). Mandatory field settings including required and optional fields can be defined for each profile. Time evaluation is a process that occurs nightly. Warning messages will be generated after this process. These warning messages should be reviewed and the appropriate action taken. For example, a warning message may indicate that an employee has exceeded their leave entitlements. Time administrators will also be required to run transaction 'CATS_DA' called 'Display Working Times' after the missing time report is corrected. The variants, or report format, to run this report showing totals by employee should be executed by the time administrator.

IMPORTANT UPDATE

R401: Inaccurate or incomplete entry of employee time data	
	S14: *Timesheets are locked for editing after submission.* After submission, the system should restrict employees from being able to edit time submitted. In order to alter time, a prior period adjustment must be processed. The ability to modify a timesheet after submission can be set within each timesheet profile. The timesheet profile should limit the number of pay periods that a time administrator can change (in both directions – forward and back). **S15:** *Automated notifications.* Automated notifications remind users to enter their time report, and continue to alert users when the time reporting deadline is reached and passed. The SAP workflow engine should be used to provide automatic notifications when time reports are due. The workflow engine enables the establishment of tolerances such as the timeframe where and when notifications sent to employees as reminders. **M55:** *Review 'Missing Time' report.* Immediately after the time reporting deadline, the payroll department should generate a report outlining missing time and follow up directly with employees and the employees' functional managers. Report: PT_EDT_TEDT – Time Statement.

R402: Unapproved leave or leave is taken outside of entitlements	
Risk type	
Consequence	Employee takes leave which is either not recorded on timesheets, or when recorded results in the employee having a negative leave balance.
Better practice	**S16:** *Automated checks on leave applications to confirm sufficient entitlement.* Use of system functionality to capture leave requests will enable comparison reporting to be generated and show any discrepancies between leave recorded in timesheets and leave requested. Time evaluation reports RPTIME00 (for positive time) or RPTQTA00 (for negative time) are also useful to identify employees with insufficient entitlements. Leave quotas and workflow rules should be established to check for appropriate leave balances prior to the leave being submitted for approval. Review System Workflow Rules (Path: Set Up HRMS, Common Definitions, Self Service, Workflow Status). **S17:** *Workflow approval of leave requests.* System functionality to process leave requests (for example, Employee Self Service) should be utilised to enable automated checks to be performed against employee entitlements and leave balances. Requested leave should route through the workflow approval hierarchy for approval prior to the request being approved. The application should be configured to raise a 'warning flag' if the requested leave will result in negative entitlement balances.

IMPORTANT UPDATE

R402: Unapproved leave or leave is taken outside of entitlements	
	The Employee Self Service component of SAP provides all of the capabilities to enable approval of employee timesheets. A worklist is provided to the approver with a list of all the absences he or she needs to approve. SAP Workflow can also be used to control the approval process. When processing and approving leave requests, SAP automatically performs a check of the employee's leave balances against the available leave quotes, and this check also takes into account other leave requests. SAP will raise a 'warning flag' if the requested leave will result in negative entitlement balances. **M56:** *Periodic review over recording of leave.* A two-way check should be performed by the payroll team on a monthly basis to confirm that: • Leave taken by employees in reflected in timesheets; and • Leave recorded was appropriately approved. Any discrepancies should be followed up with the employee and the employee's immediate supervisor. Report: Transaction PT64 – Absence Data Overview.

R403: Established employee shifts are updated inaccurately	
Risk type	
Consequence	Inaccurate employee shifts reporting may lead to inaccurate payroll processing and may impact leave accrual calculations.
Better practice	**S18:** *Restrict user access to amend employee shifts.* Access to update employee shifts should be restricted to appropriate personnel and employees should not have access to update their own shift details. Work schedules are recorded in infotype 1011 in SAP. Access to key transaction codes like HRPBSIN_ROS_MNT should be restricted to appropriate personnel. Use of authorisation object P_PERNR should be incorporated into the user's security so that no employee has access to update their own 'standard' work roster. **M57:** *Approval of updates to employee shifts.* Employee shifts should only be updated in the system following approval by an appropriate authority.

IMPORTANT UPDATE

R404: Time recorded in prior periods is amended inaccurately or without appropriate authority	
Risk type	
Consequence	Inaccurate or unauthorised adjustments lead to inaccurate leave balances or time reporting.
Better practice	**S19:** *Restrict user access to process prior period adjustment.* Access to process prior period adjustments should be restricted. This may require a procedure to be put in place whereby a manual request (appropriately approved) is submitted. There are a number of adjustment workbench transactions within SAP that can be used to manage prior period adjustments. Access to these transactions like PAUX, PAKG, PAKY, PAUY and PC00_M99_PA03_CORR must be restricted. **S20:** *Workflow approval of prior period adjustments.* Amendments to time recorded in prior periods should be processed through the workflow approval hierarchy. There are a number of adjustment workbench transactions within SAP that can be used to manage prior period adjustments. Access to these transactions like PAUX, PAKG, PAKY, PAUY and PC00_M99_PA03_CORR must be restricted. **S21:** *Limit prior period adjustments.* The system should limit the prior period for which adjustments can be processed (e.g. four weeks, or a small number of immediate past periods). SAP provides the ability to define posting periods and manage the users that can process transactions to prior periods. This is controlled through the creation of an authorisation group setting and the restriction of access to the authorisation group. It is important that access to process prior period adjustments is adequately restricted. **M58:** *Approval of prior period adjustments prior to processing.* When a prior period adjustment is required, the details are documented on a standard form requiring approval from an appropriate authority prior to processing. The adjustment is then processed in the system by a member of the payroll team. **M59:** *Review prior period adjustments.* On a monthly basis, a report should be generated that lists all prior period adjustments processed. This report should be reviewed to determine the appropriateness of adjustments processed. Report: PUOC_13 – Off Cycle Workbench.

IMPORTANT UPDATE

R405: Payroll calculation is inaccurate or incomplete	
Risk type	
Consequence	Draft payroll proposals are not reviewed for reasonableness prior to finalisation of the payroll, resulting in failure to detect significant anomalies or errors.
Better practice	**S22:** *Restrict changes and user access to modify payroll calculation rules.* Personnel calculation rules are used to calculate gross and net pay for employees and should be protected from being overridden or modified without appropriate authorisation. Heavy reliance is placed on the review of SAP exception-based payroll reports including the RPCLJNU0 – Payroll journal and RPURECG0 – run to run reconciliation report, to identify exceptions in payroll processing. **M60:** *Review payroll control reports and variance reports.* Useful reports to review prior to finalisation of the payroll include: • Payroll Exception Reports are effective where there is little variation between pay periods. Approved documentation such as leave forms, new engagements, terminations, change in pay rate, and change in deductions should be available to justify the period variation; • Payroll Budget to Variance Reports are effective in identifying significant differences; and • Employee Changes Reports highlight new employees, terminated employees and transfers to ensure only current and valid employees are included in the pay run. Once the reviewer is satisfied with the payroll calculation, a final payroll report should be produced and a copy filed. Reports: • Report S_ALR_87013611 should be reviewed by Cost Centre Managers to identify significant irregularities in payroll actual to budgeted costs. • The infotype audit report (RPUAUD00) enables the review of employee changes including new employees, terminated employees and transfers. The report can be reviewed to ensure only current and valid employees are included in the pay run. • Run to run reconciliation report (RPURECG0) enables the identification of unusual payroll results that differ from previous payrolls.

IMPORTANT UPDATE

R406: Statutory obligations for payment of taxation are breached	
Risk type	
Consequence	ATO requirements including PAYG and FBT payment requirements, are breached through failure to retain adequate records or report on and remit tax by specified deadlines, potentially resulting in penalties or reputational consequences.
Better practice	**S23:** *Restricted access to establish and amend taxation reference tables.* The ability to upload and amend tax tables within the HRMIS should be restricted and changes to reference data should be approved prior to the change being implemented. Refer to control S38 for controls operating over system patches. **M61:** *Review and approval of Fringe Benefits Tax return by appropriate authority.* The amount of FBT payable is self-assessed by the entity. Prior to lodgement of the annual FBT return, detailed review should be undertaken by an appropriate person to determine whether: • Confirmation that a fringe benefit which has been provided is accurate; and • Where a fringe benefit has been provided, the applicable rates and thresholds have been accurately applied in the calculation outlined within the return.

R407: Breach of legislative requirements relating to superannuation	
Risk type	
Consequence	Insufficient superannuation is paid, or payment is not made prior to the quarterly cut-off date. ATO guidance is contravened due to failure to retain adequate documentation in support of super contributions.
Better practice	**S24:** *Configure automated calculation of superannuation payable.* Flagging employees as eligible or ineligible for super contributions and setting the percentage of super payable should enable the super amount payable per period to be automatically calculated by referencing the payroll calculations (for salaries and wages paid) and relevant master data, such as salary sacrifice amounts and additional employee contributions. Superannuation is set up as infotype 0220 in SAP. For the payroll program to calculate the contribution amounts to any superannuation funds to which an employee subscribes, the superannuation infotype per fund for the employee must be created. Various details must be entered into infotype 0310 to enable superannuation payments including the deduction percentage and salary for superannuation purposes.

IMPORTANT UPDATE

R408: Salary sacrifice arrangements are not appropriately managed	
Risk type	
Consequence	Salary sacrifice arrangements are not clearly documented and the components are not captured in the HRMIS, leading to inaccurate taxation calculations, payments, and disbursements. Non-allowable items are included as part of a salary sacrifice arrangement. This may lead to inaccurate fringe benefits and PAYG tax calculations.
Better practice	**S25:** *Salary sacrifice details are appropriately established in the HRMIS.* The ability to establish and amend salary sacrifice details in the HRMIS should be restricted to appropriate roles within the entity, having regard to enforcing effective segregation of duty controls. Access to maintain employees' salary sacrifice is granted using the employee maintenance transactions including PA30 – Maintain HR Master Data. Access to infotype 0008 (Basic Pay) and (0589) Reimbursements must be restricted. **M62:** *Review and monitor changes to key salary sacrifice information.* Set-up of the salary package elements and rules should be independently reviewed to ensure the following: • Configuration accurately reflects the documented salary sacrifice agreement; • The salary/wage component has been accurately captured to enable accurate PAYG withholding; • Sacrifices which constitute fringe benefits have been accurately classified and captured to enable accurate Fringe Benefits Tax self-assessment; • Sacrificed superannuation is set up as an employer contribution (to be subject to taxes associated with this type of contribution) effective 1 July 2009; and • Salary package elements outside the policy framework are not included as part of the arrangement. Report: Salary sacrifice arrangements are set up as infotype and wages types records in SAP. The infotype audit report (RPUAUD00) is a useful report to identify inappropriate changes in salary sacrifice arrangements.

IMPORTANT UPDATE

R409: Methodology for performance payment is not established	
Risk type	
Consequence	Unauthorised or inaccurate bonus payments may be disbursed to employees. Bonuses may not be adequately accounted for throughout the period.
Better practice	**S26:** *Utilise system functionality to accrue for and calculate bonus payments.* Where bonus payments are based on a percentage of employee base salary or can be calculated using data established in the system, the automated accrual and payment calculation should be utilised to reduce the risk of inaccurate accrual and calculation. Where automatically calculated, the system output should be independently reviewed by an authorised HR representative for accuracy. Bonuses and rewards are typically paid through infotype 0015 within SAP. Given all bonuses and rewards are processed as one-off payments, manual controls should be implemented to review and approve all payments.

R410: Employee benefits are not managed or administered in accordance with employee agreements	
Risk type	
Consequence	Employees may receive benefits to which they are not entitled, potentially resulting in financial loss to the entity. Entity may breach terms of enterprise agreements through poor management of employee benefits process.
Better practice	**S27:** *Correctly establish and manage employee benefits.* Eligibility for employee benefits should be established by pay structure/employee role/employee type. When adding a participant, the system should be configured automatically to reference the position (if eligibility is based on level in the organisation) and should prevent participation of ineligible employees or employee classifications. If eligibility is based on information contained in master data (for example, years of service), master data should be automatically referenced to block participation of ineligible employees. Benefits are entered in the relevant benefit infotype for the employee in SAP. **S28:** *Restricted access to establish benefit plans.* Access to establish benefit plans, enrol employees, create employee specific information associated with the plan and amend plan or employee information should be restricted to appropriately authorised personnel. Access to SAP critical transactions for establishing and maintaining benefits such as HRBEN0000 (Benefits Application Menu, HRBEN0001 (Enrolment) and HRBEN0012 (Automatic plan enrolment) must be adequately restricted to authorised personnel.

IMPORTANT UPDATE

7.4 SAP controls for system maintenance and integration

The control considerations in managing and maintaining SAP should be consistent with other key business systems of the agency. Specific control elements which should be given additional consideration would include change management, interface management and business continuity management.

The management of integration between the payroll module and the General Ledger is a critical control consideration within an SAP environment. There are many SAP organisations that have had discrepancies between the General Ledger and payroll system, particularly where an SAP payroll system is interfacing into a non-SAP General Ledger system or into a highly customised SAP General Ledger.

It is important that payroll-related General Ledger accounts are established correctly and the integration settings are correct. Interface controls including reconciliation and error handling processes, must be implemented particularly where the interface is performed to a non-SAP General Ledger system.

Payroll structures

To calculate the payroll, SAP uses the following:

- Conditions, awards and rules which are stored as payroll schema;
- Wage types which are used within SAP to record different payment types including basic pay, and overtime and so on;
- Employee master records including pay rates and conditions, and organisation chart information, which can determine awards and conditions; and
- Exception-based transactions including timesheet entry.

Key control objectives

Control objective	Risks mitigated
Payroll information is completely and accurately posted to the General Ledger via the payroll journal.	**R501:** Payroll system does not reconcile to the General Ledger.
Information regarding superannuation contributions is submitted to superannuation funds (such as ComSuper) via an automated interface, ensuring complete and accurate transfer of data.	**R502:** Incomplete or inaccurate submission of superannuation data.
The rate at which leave accrues and leave types to which employees are entitled is accurately established.	**R503:** Leave accrual rates are established inaccurately.
Fields requiring translation into a foreign currency correctly reference accurate foreign exchange rates within the HRMIS to enable accurate calculations.	**R504:** Employee wages paid in foreign currency are calculated incorrectly.
The organisational chart within the application is continuously maintained to accurately reflect vacant and filled positions within the entity, assisting with position management and recruiting efforts.	**R505:** The HR system organisational chart does not accurately reflect current employees and their position.

IMPORTANT UPDATE

Payroll schemas and business processing rules are comprehensively and accurately established to enable a stable payroll calculation requiring minimal manual intervention, and are protected from unauthorised modification.	**R506:** Payroll schemas established or modified inaccurately or without authorisation.
Risks to business systems are generally reduced when available patches are installed in a timely manner after being tested for reliability and usability.	**R507:** Application is vulnerable to security or availability threats.

Risks and controls

R501: Payroll system does not reconcile to the General Ledger	
Risk type	
Consequence	The payroll system should reconcile to the General Ledger to ensure integrity of the financial statements. If not reconciled, or reconciled incorrectly, there is an increased risk of material misstatement in the financial statements.
Better practice	**S29:** *Utilise auto-posting functionality.* Where auto-posting functionality is available within the application, it should be utilised to update the General Ledger. Appropriate configuration between the systems is required, and this should be manually triggered so that only final approved payroll results are updated to the General Ledger. The calculation of the payroll system accrual depends on the establishment of wage types and General Ledger accounts. Each wage type must be allocated to the relevant General Ledger account. Effective allocation of wage types to General Ledger accounts is important for the accuracy of the payroll system accrual. The posting to accounting: payroll results not posted report (RPCIPCO0) should be regularly reviewed. **M63:** *Review of payroll posting results.* A review of payroll results that have not posted to the General Ledger should be performed at each pay cycle. If payroll transactions are manually posted (or a file manually uploaded into the General Ledger), a reconciliation should be performed and payroll that is not posted should be actioned. Report: The posting to accounting – payroll results not posted report (RPCIPCO0) should be regularly reviewed.

IMPORTANT UPDATE

R502: Incomplete or inaccurate submission of superannuation data	
Risk type	
Consequence	Information submitted to the superannuation fund is incomplete or inaccurate, potentially leading to penalty payments or incorrect reporting of superannuation payments.
Better practice	**S30:** *Superannuation data is provided in the required format and in the required timeframes.* Superannuation data should be provided in the required format and in the required timeframes as defined by the relevant recipient. Where available, the entity should generate such reports and data from the payroll system data. Submission of superannuation contributions is typically performed through either electronic files and/or reports produced by SAP. Manual controls are typically relied upon to reconcile amounts paid with superannuation amounts reported by SAP. **S31:** *Changes to superannuation interfaces and data file formats are managed using entity IT change management controls.* Changes and upgrades to the HRMIS should not inadvertently modify customised interfaces or data files. This is not an automated control within SAP.

R503: Leave accrual rates are established inaccurately	
Risk type	
Consequence	Inaccuracies in leave accruals reduce the accuracy and reliability of the payroll calculation and associated financial reports.
Better practice	**S32:** *Manage leave accrual rules.* Leave accrual rules are used to calculate employee leave accruals. The leave accrual rules should be consistent with employee conditions for employment (and/or employee agreement) and linked within the application to employee entitlement information. Leave provisions are set up within SAP customising at the following path —Payroll: Australia/Leave Provisions and Payments/Leave Provisions. Leave provisions must be appropriately set to enable effective and accurate calculation of leave accruals. Infotypes such as Absence Quotas (2006), Planned Working Time (0007), Basic Pay (0008) and Contract Elements (0016) must also be used to enable accurate calculation of leave accruals. **S33:** *Configuration of maximum values for leave accruals.* If employee conditions of employment specify a maximum amount of leave which can be accrued or carried forward, maximum values should be configured for each type of leave accrual. If the maximum leave accrual amount is reached, an error message should be reported and the system designed to stop accruing further leave. Employee leave entitlements are set up as wage types in SAP. Maximum values can be set in each of the appropriate wage types for each type of leave accrual. If the maximum leave accrual amount is reached, SAP will stop accruing leave for the employee.

IMPORTANT UPDATE

R503: Leave accrual rates are established inaccurately	
	M64: *Regular review of employees' leave accruals should be performed.* A manual review of employee's leave accruals should be performed by managers to assess for reasonableness against known periods of leave taken by employees. A further review should be performed by HR to identify any excessive or negative balances. Report: RPILVA00 (Leave Accruals) can be used to manually review of employee's leave accruals. The review should be performed by Cost Centre Managers to assess for reasonableness against known periods of leave which employees have taken. A further review should be performed by HR to identify any excessive or negative balances.

R504: Employee wages paid in foreign currency are calculated incorrectly	
Risk type	$
Consequence	Use of inaccurate foreign exchange rates for currency translation purposes will result in inaccurate calculation of payroll.
Better practice	**S34:** *Establish automated updates for foreign exchange rates.* An automated update of foreign exchange rates should be established with an authorised source and the entity application to ensure rates applied are up to date and accurate. There are numerous programs like RFIMPNBS that facilitate the automatic upload of currency rates. Organisations configure and use SAP differently to calculate and pay employees in foreign currencies. One useful functionality item is the use of employee sub-groups for employees that are paid in foreign currencies. Reliance is placed on the review of SAP exception based payroll reports including the RPCLJNU0 – Payroll journal and RPURECG0 – run to run reconciliation report to identify foreign currency exceptions in payroll processing.

IMPORTANT UPDATE

R505: The HR system organisational chart does not accurately reflect current employees and their positions	
Risk type	
Consequence	Incomplete organisation chart may impair the accuracy of workflows associated with self-service functionality, and user access privileges. Other impairments include headcount errors and incorrect workforce planning decisions.
Better practice	**S35:** *Restricted access to update organisational chart.* Access to update the organisational chart should be restricted to appropriate personnel. Amendments should only be processed based on appropriately approved documentation (for example, authority to create a new position). The effective establishment and maintenance of the SAP organisation structure is critical to the control environment. If position-based security is used user access is allocated based on a user's position and/or job in the organisation structure. Access to maintain the organisation structure through transactions such as PO03 and PO13 must be restricted. All changes to the organisation structure should be documented, appropriately approved and reviewed for appropriateness. **S36:** *Ability to display temporary assignments.* Functionality enabling the organisational chart to display temporary assignments should be utilised to enable tracking of higher duties assignments. The organisation chart functionality in SAP provides the ability to manage and display higher duty assignments. **S37:** *Organisational chart designed to reflect the hierarchy.* The organisational chart should be designed to reflect the hierarchy for each department or organisational unit. The effective establishment and maintenance of the SAP organisation structure is critical to the control environment. If position-based security is used user access is allocated based on a user's position and/or job in the organisation structure. Access to maintain the organisation structure through transactions such as PO03 and PO13 must be restricted. All changes to the organisation structure should be documented, appropriately approved and reviewed for appropriateness.

IMPORTANT UPDATE

R506: Payroll schemas established or modified inaccurately or without authorisation	
Risk type	
Consequence	Payroll accuracy is impacted as a result of errors caused by the incorrect set-up of payroll schemas or rules that cause the schemas to execute calculations inaccurately.
Better practice	**S38:** *Access to establish or modify payroll schemas or elements and rules is restricted.* Access to set up or modify payroll schemas or elements and rules should be restricted to appropriate personnel. Within SAP, access to the following functions and transactions codes must be adequately restricted: • Access to maintain the payroll schema through transactions PE01 and PE02. • Access to maintain wage types using transaction PU30. • Access to payroll configuration settings in the IMG using transaction SPRO.

R507: Application is vulnerable to security and availability threats	
Risk type	
Consequence	A software update is not installed in a timely manner or not installed completely and accurately, making the application vulnerable to security breaches and threatening the availability of the application.
Better practice	**S39:** *Automatic notification of available software updates.* Automatic notification should be configured to alert the system administrator whenever a software update is available. SAP provides automatic notifications of new software releases and patches through its service market place. SAP Administrators have accounts to the market place and are able to download the required updates and patches. **M65:** *Timely installation of approved software updates.* All software updates should be tested in a controlled environment (replicating the production environment) before being released into production.

IMPORTANT UPDATE

7.5 Useful reports for SAP Human Capital Management

The *SAP Human Capital Management module* provides standard reporting functionality. The table below provides a list of specific reports to the HR functions that are useful tools for both management decision making and internal controls. The list does not include customised reports which will be different for each agency.

Code	Name	Description
HR and payroll data management		
S_AHR_61016503	Staff Assignments	Listing of staff assignments per payroll group and subgroup.
S_AHR_61016528	Structure Display/Maintenance	Overview of payroll structure per payroll group and subgroup.
S_AHR_61016531	Display and Maintain Infotypes	The report provides an overview of infotype, including employee master data changes.
S_AHR_61016360	Master Data Sheet	Listing of employee master record details including personal and bank information. This report is useful from a control perspective for identifying ghost employees.
RPUAUD00	Infotype Audit Report	Highlights all changes to critical infotypes as defined in configuration. Critical report to identify inappropriate changes to master data.
PT91; PT91_ATT	Absence/Attendance Data: Multiple Employee View	This report allows you to summarise and classify your employees' attendances and absences from various points of view. The data is displayed in a list. You can display leave data for employees for a particular personnel area sorted according to personnel sub area and employee. This report is useful in identifying inappropriate leave data.
RPILVA00	Leave Accruals	Outlines each employee's leave accrual. This report can identify employees' with large and inappropriate leave balances.
PT_ETD_TEDT	Time Statement	Report RPTEDT00 creates an overview of the results determined by time evaluation, for example, an overview of time balances and time wage types for each employee. You can use the report to check the time evaluation results, for example, or to send time statements to employees.
PC00_M01_CEDT	Remuneration Statement	Listing of employee deductions per pay run.
PC_PAYRESULT	Display Results	Report provides a basic overview of the organisation's employee pays and deductions.

Part 2: System-specific Controls

IMPORTANT UPDATE

Code	Name	Description
Employee commencement		
S_AHR_61016376	Employee List	List of all employees recorded within the HR organisation. This report is useful in displaying new employee commencements.
RPUAUD00	Infotype Audit Report	Highlights all changes to critical infotypes including new employee listings.
Position management		
AQZZ/SAPQUERY/ H2STAFF_CHANGES2	Headcount Change report	The Headcount Change report creates a list of personnel actions that have been performed for employees in the selected period. This report would assist in highlighting transfers in and out of agencies.
RPLTRF00	Time Spent in Each Pay Scale Area/Type/ Group/Level	This report display the assignment to wage level and the time spent in pay scale group/level of the individual employees. This report can assist with ensuring employees are being paid at the correct rate, particularly if they have undertaken higher duties or worked in a different position for a period of time.
RHXSBES0	Staff Assignments	This report displays the relevant staff assignments for one or more organisation units with a staffing percentage and approval and employment hours. This can assist in determining whether time has been split appropriately between positions/ organisational units.
Employee exits and terminations		
PC00_M40_TERM	Termination Workbench	The termination workbench provides the ability to report all termination payment items.
RPUAUD00	Infotype Audit Report	Highlights all changes to critical infotypes as defined in configuration. Employee terminations would be reported on the infotype audit report.
Time reporting		
RPLTRF10	Time Spent in Pay Scale Group/Level	This report can be used to check that employees have accurately recorded higher duties.
RPTABS60	Attendance/Absence Data – Multiple Employee View	A useful high-level report for reviewing reasonableness of employee time data. Other standard reports enable one to drill down into individual employees; attendance only; absence only and so on.

IMPORTANT UPDATE

Code	Name	Description
Payroll processing and administration		
RPCEDTD0	Remuneration statement	The remuneration statement provides an overview of the payments and deductions for each employee per payroll run.
RPCLJNU0	Payroll journal	The payroll journal contains selected, detailed payroll data for multiple employees that have been created during a specific period or during a selected payroll period. The journal can be used to identify errors during the payroll run, to total payroll data for a cost centre, or as a controlling report checking. The payroll journal can be structured according to the entity's requirements.
H99_DISPLAY_PAYRESULT	Display Payroll Results	The Display Payroll Results report displays the payroll results that pertain to one or multiple personnel numbers.
RPURECG0	Run to Run Reconciliation Report	This reconciles the year-to-date figures for the last payroll period with the figures for the current payroll period, and generates new year-to-date figures for gross pay, tax, untaxed deductions and the number of employees paid. The report can be scheduled to run automatically after a payroll run.
PC_PAYRESULT	Display Results	This displays employees' total hours, earnings, allowances, taxes and deductions for the current payroll period, the month-to-date and the year-to-date. The amount paid, retroactive calculations and gross pay are only displayed for the current payroll period.
HRBEN0071	Eligible Employees	Shows the employees who are eligible for specified benefit plans on a given date. The report is run for a key date (today's date or another date).
HRBEN0072	Benefit Plan Participation	This report shows the employees who are participating in specified benefit plans on a given date or during a certain period of time.
HRBEN0077	Changes in Benefit Elections	Shows the changes made to benefit plan infotype records on a given date or during a certain period in time. These changes include new enrolment, termination, or changes in the employee elections for a plan.
HRBEN0079	Changes of Eligibility Status	Shows employees who are no longer eligible for the plans in which they are participating.

IMPORTANT UPDATE

Code	Name	Description
HRBEN0083	Changes in General Benefits Information	Detects deviations from system-allocated default values in an employee's General Benefits Information (infotype 0171).
HRBEN0087	Benefit Election Analysis	This report shows percentage changes in plan participation and eligibility for plans between two given dates. It enables you to assess the popularity of individual benefit plans offered by your organisation in order to help you make decisions about the palette of benefits that will offer in future.
HRBEN0076	Contribution Limit Check	During enrolment, the system automatically takes the contribution limits defined in Customising into account, and only allows employees to choose contributions that are within these limits. After enrolment, however, an employee's contributions can become invalid if a new different contribution rule becomes valid for an employee. This report detects employee contributions (stored on the plan infotype as an amount, percentage of salary, or as units) that are not within the limits on a key date. It is particularly useful for checking the contributions of employees who become classified as highly compensated after enrolling in a plan that has different limits for highly compensated and non-highly compensated employees. You therefore need to run the check report after the annual process of identifying highly compensated employees in order to detect employees who must change their contributions.
System maintenance and integration		
RPDASC00	Changes to personnel calculation rules	Personnel calculation rules determine employee payments. This report should be reviewed whenever changes are processed.

IMPORTANT UPDATE

8. Aurion – Human Resources and Payroll Management

The chapter provides detail on the risks and controls by HR function as managed by Aurion's human resources and payroll management.

8.1 Aurion controls for HR and payroll data management

Employee information stored as master data is fundamental to the Aurion's handling of the HR and payroll processes. The nature of such information is sensitive and subject to privacy and legislative requirements and therefore should be adequately controlled.

The Jobs & People module is the core module within the Aurion system. All people are recorded in this module first as a Person, then optionally as an Employee. Aurion assigns a Person Number to all people including external people such as contractors and training providers. This number is different from the Employee Number, which is only assigned when a person is commenced on the Payroll or Leave modules.

Most of the modules in Aurion require codes that the Aurion Coordinator maintains in the Aurion code tables.

People can be managed in the web client or in client-server. The web client also provides access for all employees to the My Aurion portal where they can view and update their own details.

Key control objectives

Control objective	Risks mitigated
HR and payroll data is appropriately maintained to provide accurate and complete employee information and payroll transactions	**R201:** HR master data is inaccurate. **R202:** HR master data is not secure.

Risks and Controls

R201: HR master data is inaccurate	
Risk type	
Consequence	Employee details may be incorrectly entered or maintained, which may result in duplicate payments, errors with superannuation contributions or employee deductions, or unapproved changes to the allocation of roles and delegations.
Better practice	**S01:** *Define key data entry fields.* Key data fields should be defined in the system to confirm that information necessary to the completion of master data is entered. Aurion has programmatic controls in place that make recording certain data items mandatory via the Client Server interface. Additional fields can be marked as mandatory using the task ES767_BOIL_LIST – Boilerplate Control. Employee Self Service access can be configured so that any data entry field can be marked as mandatory even if the underlying coding does not require it. This is controlled in the Aurion Repository by marking the fields Optional column as NO.

IMPORTANT UPDATE

R201: HR master data is inaccurate	
	If required an automated reporting solution utilising Aurion's internal Business Process Automation (BPA) can be configured that will report back to the user, or any other recipient, where a particular data item is incorrect or missing. **S02:** *Restricting user access to view, establish and update master data.* Access to view, establish and update master data should be restricted to appropriately authorised users. Users with the ability to view master data should also be appropriately restricted to reduce the likelihood of inappropriate viewing or distribution of data. Information in Aurion has been compartmentalised into individual 'tasks' and each task can be secured on an individual basis. A group of tasks can be combined into a profile and these profiles can be assigned to a user, position or organisation unit as needed. Profiles can be created using task ES651_SECPR_TREE – Profiles. Assign the profiles to Users via ES007_SEC_USER – Users and to Positions or Org units using ORG_POS_SECURITY – Org & Position Security. The ability to access an individual's records via the profiles can further be restricted based on the organisation unit access and this can also be assigned to a user, position or org unit with the same tasks above but using the Process – Security Access pulldown. Most tasks also have a view only equivalent and these can be easily identified as they have 'View' in the task description. Users can be prevented from accessing their own records in Client Server mode via a system wide control. This is enabled using the Restrict Standard Select Self checkbox in the ES010_SYS_CONT – Control Record. In Employee Self Service all relevant fields can be made updateable, read only or hidden and this can be applied to the employee, supervisor or administrative user. This is performed in the Aurion Repository using the Availability, Self-Access, Supervisor Access and Other Access columns. **S03:** *Validation checks on certain fields warn the user that the information is duplicated in another employee record.* Validation checks should be configured to decrease the likelihood of inaccurate information being entered (for example, tax file number cannot be duplicated in another employee record). On commencement of an employee Aurion performs a validation check to see if there is replication on certain fields and if a potential duplicate is found prompts the user to check before proceeding. Utilising Aurion's internal reporting tool, Aurion Query Tool (AQT), it is also possible to report on duplications found in any data field. Aurion also has a standard report (ER150_DUP_EMP) that checks for Duplicate Employee data. **M50:** *Establishment and amendment of master data occurs only when supported by appropriately approved documentation.* All master data established and all amendments processed to master data should be supported by appropriate documentation (approved by an appropriate authority where relevant). Report: Masterfile Changes Report ER432_MST_SNAP.

IMPORTANT UPDATE

<table>
<tr><th colspan="2">R202: HR master data is not secure</th></tr>
<tr><td>Risk type</td><td></td></tr>
<tr><td>Consequence</td><td>Unauthorised users may have access to view and maintain sensitive HR and payroll data, which may compromise the confidentiality of personnel records and may also result in the processing of fraudulent payroll payments.</td></tr>
<tr><td>Better practice</td><td>S04: Access to HR master data is appropriately configured and managed.

Implementing appropriate user access controls requires:
• Identification and implementation of segregation of duty requirements in relation to validating updates/modification/deletion of master data within the HRMIS is complete and appropriately authorised;
• Access to the application and to underlying data (such as the database) is assigned based on user profiles and/or roles; and
• Employees should be limited in their ability to modify reference data items (salary, leave records and employment date) for their own records. With Web Client applications—like employee self-service (ESS)— the client may allow an employee to be able to modify their own data with the exception of high-risk data fields, including salary, hourly rate, additional pay, job grade.

Access controls provide appropriate restrictions to user access to certain data types. Access should be controlled at three levels:
• Restrict access to appropriate users (for example, HR personnel but in some situations access may be wider if ESS is implemented);
• For each authorised user, restrict access to particular types of master data (for example, only some authorised users will have access to bank details); and
• For each user and each type of data, specify whether access is ‘view’ or ‘edit’ access.

As referenced previously, information in Aurion has been compartmentalised into individual ‘tasks’ and each task can be secured on an individual basis. A group of tasks can be combined into a profile and these profiles can be assigned to a user, position or organisation unit as needed. Profiles are created using ES651_SECPR_TREE.

The ability to access an individual’s records via the profiles can further be restricted based on the organisation unit access and this can also be assigned to a user (ES007_SEC_USER), position or org unit (ORG_POS_SECURITY).

Most tasks also have a view only equivalent which are generally start with the word ‘View’ in the description.

Some data, such as completed (paid) Payroll records, cannot be modified at all.

Users can be prevented from accessing their own records in Client Server mode via a system wide control, specifically the ‘Restrict Standard Select Self’ checkbox in the Control Record (ES010_SYS_CONT).

In Employee Self Service all relevant fields can be made updateable, read only or hidden and this can be applied to the employee, supervisor or administrative user.

S02: Restricting user access to view, establish and update master data is also relevant.</td></tr>
</table>

IMPORTANT UPDATE

R202: HR master data is not secure	
	M51: *Review of system configuration reports.* Generally system configuration change reports are available from the HRMIS and may be reviewed periodically to monitor changes to key controls or configuration settings. Such reports should be run periodically. Consideration should be given to ensuring that appropriate 'audit' tables and associated logs are also configured. Failure to configure such tables may mean that important information is not available for inclusion in monitoring reports. Report: ER539_AUDIT_EXP (Audit Output Enquiry) – This report enables you to make a selection of audit records that can be output to a file and then used as input to a desktop application for further analysis. The format of the records included in the output file is dependent upon the entity selected. Each record in the output file contains the old value, new value and a change indicator text (if specified) for audited entity fields. Options on the parameter form allow you to reduce the number of columns in the output text file by selecting the Summary of Changes only checkbox and/or the Output only field changes for 'MODIFY' events? checkbox.

8.2 Aurion controls for workforce management

Key control considerations in Aurion that relate to workforce management include implementing appropriate user access security settings as well as appropriate configuration control settings that are line with legislation and compliance requirements. User access controls implemented via permission lists and roles helps monitor whether access to workforce management is restricted according to organisational requirements.

The Jobs & People module manages core information about an organisation's structure, positions and people, with full history. This allows a complete picture of the skills and experience of the workforce, including contractors and volunteers, which in turn allow easy calculation of the full cost of delivering a product or service. This module allows HR staff to start and cease employees in the organisation.

'Jobs & People' provides the foundation for Aurion to automate other business processes including placements, cost allocation, workflow, and security and reporting. Workforce planning tools, including customised query and reporting tools, provide analytic capability.

The Workforce Budgeting module tracks expenditure against salary budget and alerts to significant variation from forecasts using tolerances that the user defines. Aurion alerts to significant variation from forecasts using tolerances that are defined by the organisation. Flexible drilldown enables the identification of the reason for the change and assess corrective action.

Key control objectives

Control objective	Risks mitigated
Appropriate and accurate employee information is collected and maintained.	**R301:** Non-existent or duplicate employee is added to the payroll. **R302:** Termination payments and balances are inaccurately calculated. **R303:** Employee is not deactivated when employment is terminated.

IMPORTANT UPDATE

Risks and Controls

R301: Non-existent or duplicate employee is added to the payroll	
Risk type	
Consequence	‘Ghost’ or duplicate employees on the payroll lead to overpayment or processing of fraudulent payments.
Better practice	**S05:** *Access to add an employee should be restricted to appropriate individuals and segregated from payroll maintenance.* Access to modify employee information should be restricted to decrease the likelihood of inappropriate or unapproved changes to employee information which may impact upon the accuracy and completeness of information maintained in the HRMIS. Additionally, restricting access in accordance with privacy principles reduces the risk of inappropriate disclosure of employee information. The ability to update or add records is based on individual tasks which can be grouped into specific profiles. Using this type of configuration it is possible to secure separately the ability to: • Add/change establishment data • Add new employee record, or • Amend existing employee record In addition it is possible to secure different organisational units within each of the access types. Access to the org unit security is made via the Process – Security Access facility from the ES007_SEC_USER and ORG_POS_SECURITY tasks. Aurion can also report on any field within the database so that automated cross referencing or third party review of information is possible using only the installed software. *Also refer to **S03:** Validation checks on key fields warn the user that the information is duplicated in another employee record.* **M52:** *When adding a new employee, a listing of current employees should be reviewed to reduce the risk of duplicating the employee record.* A system report of all current employees should be generated prior to adding a new employee, and checked to confirm the employee does not already exist in the system. A system report of all new employee additions should be generated monthly and an individual who is independent from the employee set-up process should check each addition against supporting paperwork (for example, approval to engage, employee information including bank account) to validate the set-up was authorised and has been completed accurately. Report: ER150_DUP_EMP – This report lists groups of employees that have similar details to another employee. An employee is categorised as a duplicate for the original employee when they have the same Tax File Number or when three of the following details are the same; Surname, First name, Gender, Date of birth.

IMPORTANT UPDATE

R302: Termination payments and balances are inaccurately calculated	
Risk type	
Consequence	Termination payment is incorrect, resulting in incorrect salary and leave entitlements being paid or reported
Better practice	**S06:** *Application will warn user if termination date in the past is entered.* The system should be configured such that if a termination date in the past is entered, a warning message is generated to reduce the occurrence of backdating of terminations and to accurately process termination payments and calculations. Aurion does not specifically warn when a termination date in the past is entered as it is common to process a termination only after all relevant documents or updates have been received (for example, final flex balance, outstanding leave forms etc). Information such as the final flex balance could only be received after the employees last day of work and therefore after the termination date. However Aurion does warn when the termination date would require any of the following items to be amended or reversed: • Existing Payroll transactions • Timesheets, or • Leave entries. **S07:** *Workflow operates to require independent approval verification of termination date entered.* Automated workflow approvals utilising organisation hierarchy positions delegations of authority should be utilised to approve terminations. The approver should verify the termination date of the employee prior to approving. It is possible to create an electronic form in Aurion using Setup SS Forms (SURVEY_X5) that would record the relevant approval or clearance from various sources including the confirmation that the termination date is correct. This Workflow (ES688_WFLOW_TREE) can be based on the existing organisation and position reporting structure. **S08:** *Application automatically calculates payments based on master data, termination date entered, and leave entitlements.* Use of system functionality to calculate and report entitlements and balances is more accurate. The effectiveness of this control requires accurate data entry and maintenance of employee information and master data. Aurion automatically calculates final monies including leave entitlements and tax treatment. In addition it is possible to configure additional termination payments, such as voluntary redundancy payments, which trigger based on the termination reason using Severance Pay Rules (ES927_SEVRL_LIST). **M53:** *An independent authority checks the termination date per notification documentation to the date entered in the system.* On a monthly basis, a report of all terminations is generated and an individual who does not have access to terminate employees checks that all termination dates were accurately entered, with reference to termination documentation (for example, resignation letter).

IMPORTANT UPDATE

R303: Employee is not inactivated when employment is terminated	
Risk type	
Consequence	Employee record is not flagged as terminated which may result in subsequent payment to the employee. For agencies using 'single sign on' (which enables access to all applications without requiring separate passwords, by using credentials at the network sign-on level), failure to inactivate terminated employees may also fail to inactivate network access.
Better practice	**S09:** *Application automatically changes status of employee to 'terminated' as at termination date entered.* Systems are configured to automatically change the status of employees to 'terminated' as at the entered termination date. This is typically enabled through automated batch processing. An employee is automatically changed from 'Active' to 'Terminated' when a termination record is created. Aurion also inhibits the employee's security profile on termination. **S10:** *Application automatically disables terminated employee's access to systems based on termination date entered.* This control is possible where position-based security is utilised. Appropriate use of the termination date is important where single-sign access is granted based on a commencement or termination date. An employee's User ID is automatically made inactive when a termination is processed. In addition, if security access is position based the system does not recognise the employee as occupying the position after termination and will therefore prevent access. **S11:** *Application does not allow payment to be disbursed to employees with 'terminated' status.* Operation of this control typically does not require specific configuration within the system, as it is deemed 'standard' functionality. It may be possible in some circumstances to process ad-hoc payments to terminated employees using some applications In the termination pay (i.e. the pay in which the termination is processed) Aurion allows normal functionality but post termination a manual pay record would need to be created before any ad-hoc payment could be made using the Process – Pay Record Management – Create Pay Record function from the Pays tab of the Payroll workbench (ES805_PAY_TABCTL). Aurion's trial pay and payrun report (ER368_PAYRUN) both have a standard alert that a terminated employee is receiving a payment. **M54:** *Department/Cost Centre managers are periodically provided with a listing of employees for which they are responsible. This listing is checked to determine whether it contains any employees no longer working within the department.* System generated listings of current employees per department/area/cost centre should be provided to relevant managers to verify current employees. This check assists in detecting employees who have transferred or been terminated and information regarding the transfer or termination has not been recorded in the system. Report: ER076_ORG_STAFF – This report provides a summary of organisation units, positions, placements, actual placements and, if required, unattached staff. Full-Time Equivalent details are also reported in the Remarks column for part-time employees, and full-time employees where the full-time equivalent is not 1. The report identifies placement vacancies and actual placement vacancies, and is used to control temporary arrangements and consequential vacancies. All positions in an organisation unit are reported, in classification sort order (that is, highest paid at top). You may optionally select to include unattached staff in the report. You may also specify Employment Types that are to be excluded from the report. If an employee's Employment Type for the placement is one of the specified codes, they will not appear on the report.

IMPORTANT UPDATE

8.3 Aurion controls for payroll processing and administration

Aurion's payroll module manages the payment and disbursement of salary and other entitlements for employees. Aurion uses the Award Interpreter module to define the conditions of employment for an employee. These are set up to reflect the way the organisation does business. The Leave module describes the employee's leave and other entitlements while the Timekeeper module describes the number of hours the employee works each day.

Integrating 'Payroll' with 'Award Interpreter' allows consistent interpretation of award conditions without user intervention. Integrating 'Award Interpreter' with 'Timekeeper' and 'Leave' allows time and attendance processing to be fully automated.

Key control objectives

Control objective	Risks mitigated
Evidence of employee service and time is accurately recorded in the appropriate period.	**R401:** Inaccurate or incomplete entry of employee time data. **R402:** Unapproved leave or leave is taken outside of entitlements. **R403:** Established employee shifts are updated inaccurately. **R404:** Time recorded in prior periods is amended inaccurately or without appropriate authority.
Evidence of employee service and time is accurately recorded in the appropriate period.	**R405:** Payroll calculation is inaccurate or incomplete.
Evidence of employee service and time is accurately recorded in the appropriate period.	**R406:** Statutory obligations for payment of taxation are breached. **R407:** Breach of legislative requirements relating to superannuation. **R408:** Salary sacrifice arrangements are not appropriately managed.
Evidence of employee service and time is accurately recorded in the appropriate period.	**R409:** Methodology for bonus rewards is not established. **R410:** Employee benefits are not managed or administered in accordance with Workplace Agreements/employee contracts.

IMPORTANT UPDATE

Risks and controls

R401: Inaccurate or incomplete entry of employee time data	
Risk type	
Consequence	Time data entered does not accurately reflect time worked or does not include leave taken. Employee receives payment for hours or leave to which they are not entitled.
Better practice	**S12:** *Workflow approval of employee time.* Where workflow functionality is used, such as in self-service, the workflow should be configured so that submitted employee time is automatically routed through the workflow approval hierarchy for review by the employee's immediate supervisor or functional manager. The workflow should also be used to send rejected time allocations or leave requests to the employee via the system with the reason recorded. Where Aurion's internal timesheet recording and interpretation (Timekeeper) is in use, the system routes approval based on the existing establishment setup. The workflow is configurable (ES688_WFLOW_TREE) and can be made to route differently based on: • Organisation Unit • Company • Pay Entity (a group of employees), or • Award (employees with the same entitlements). The workflow can be used to send back a timesheet that needs amending. Leave entries must match the timesheet or the approval workflow will not be able to be commenced. **S13:** *System validation of data entered.* Validation checks should be configured to decrease the likelihood of inaccurate time being entered (for example, minimum/maximum number of working hours, checks against established time codes). The system may also be configured to provide default timesheets to employees with standard responsibilities and working hours. Timekeeper allows for a fully configurable set of validation checks to be performed. Checks can be based on min/max hours, time of day, day of week or combinations thereof. Default timesheets can be created and rolled out for a group of employees or on an individual basis. **S14:** *Timesheets are locked for editing after submission.* After submission, the system should restrict employees from being able to edit time submitted. In order to alter time, a prior period adjustment must be processed. After submission, but before approval, an employee cannot change a timesheet but can recall it. If recalled, an alert is sent to the relevant supervisor. After approval but before payment a timesheet can only be changed via the Client Server interface using the Timekeeper tab (ET150_TK_LIST) on the Payroll Workbench. After a timesheet has been paid it is not possible to change it at all and an adjustment line must be added to a following period.

IMPORTANT UPDATE

R401: Inaccurate or incomplete entry of employee time data	
	S15: *Automated notifications.* Automated notifications remind users to enter their time report, and continue to alert users when the time reporting deadline is reached and passed. A standard automated message is sent to a supervisor when a timesheet has been submitted but not yet approved. It is possible to create automated messages to the employee or supervisor utilising Business Process Automation (BPA) that alerts on timesheets in any specified condition. There is also a standard Aurion report that shows the current condition of timesheets (ER067_TK_PROCESS). **M55:** *Review 'Missing Time' report.* Immediately after the time reporting deadline, the payroll department should generate a report outlining missing time and follow up directly with employees and the employees' functional managers.

R402: Unapproved leave or leave is taken outside of entitlements	
Risk type	
Consequence	Employee takes leave which is either not recorded on timesheets, or when recorded results in the employee having a negative leave balance.
Better practice	**S16:** *Automated checks on leave applications to confirm sufficient entitlement.* Use of system functionality to capture leave requests will enable comparison reporting to be generated and show any discrepancies between leave recorded in timesheets and leave requested. Leave applications must be processed in the applicable self service or client server area. The leave application is then cross referenced to the timesheet and where they do not match the timesheet cannot be processed. Leave applications that do not have a sufficient entitlement cannot be processed **S17:** *Workflow approval of leave requests.* System functionality to process leave requests (for example, Employee Self Service) should be utilised to enable automated checks to be performed against employee entitlements and leave balances. Requested leave should route through the workflow approval hierarchy for approval prior to the request being approved. The application should be configured to raise a 'warning flag' if the requested leave will result in negative entitlement balances. Leave applications can only be entered in Self Service where the pre-set rules regarding balances and/or length of application are adhered to. Applications can be routed based on the leave type or length of absence while still following the establishment hierarchy. Different leave types can be forced to have an approval from a higher delegated authority which is directly related to the position.

IMPORTANT UPDATE

R402: Unapproved leave or leave is taken outside of entitlements	
	M56: *Periodic review over recording of leave.* A two-way check should be performed by the payroll team on a monthly basis to confirm that: • Leave taken by employees in reflected in timesheets; and • Leave recorded was appropriately approved. Any discrepancies should be followed up with the employee and the employee's immediate supervisor. Report: EV523_LVE_ENQIRY – This report details employee leave occurrences, placements, people and employment information. Leave attributes are nominated that are required to satisfy the specific enquiry. Attributes that can be selected include: • Who – Employee, Organisation Unit/s • Dates of leave – Date Range, Leave Starting/During/Ending • Optional Leave characteristics – Leave Type, Approval Status, EEO Details.

R403: Established employee shifts are updated inaccurately	
Risk type	
Consequence	Inaccurate employee shifts reporting may lead to inaccurate payroll processing and may impact leave accrual calculations.
Better practice	**S18:** *Restrict user access to amend employee shifts.* Access to update employee shifts should be restricted to appropriate personnel and employees should not have access to update their own shift details. Access to amend a recorded roster or work pattern is restricted to client server access with controls as per previous sections. The Change Employee Status task (ES229_CES_DRV) or the Status tab (ET104_EMP_DET03) from the Person Workbench (ES313_BIO_TABCTL) can be used to record these details. **M57:** *Approval of updates to employee shifts.* Employee shifts should only be updated in the system following approval by an appropriate authority. Reports: ER090_MAN_CONT – This report details the hours and amounts processed for employees in a nominated pay entity or organisation unit, and within a range of specified dates. ER030_USER_RPT – The object of this report is to list Security Users and, for each User, provide details of their respective Employee Details, User Profile and User Access. One or more Location codes may be optionally entered, to restrict reporting to that/those location/s.

IMPORTANT UPDATE

R404: Time recorded in prior periods is amended inaccurately or without appropriate authority	
Risk type	
Consequence	Inaccurate or unauthorised adjustments lead to inaccurate leave balances or time reporting.
Better practice	**S19:** *Restrict user access to process prior period adjustment.* Access to process prior period adjustments should be restricted. This may require a procedure to be put in place whereby a manual request (appropriately approved) is submitted. Prior period adjustments are recorded on a separate section of the timesheet and time types available in this section are configurable via the Timekeeper Ruleset Maintenance task (ES815_TKRUL_TREE). In most cases the amendments need to be processed manually via the client server interface. **S20:** *Workflow approval of prior period adjustments.* Amendments to time recorded in prior periods should be processed through the workflow approval hierarchy. Amendments to timesheets are approved in the same manner and at the same time as the normal timesheet and therefore are subject to the normal workflow as configured in the Workflow Ruleset Maintenance task (ES688_WFLOW_TREE). **S21:** *Limit prior period adjustments.* The system should limit the prior period for which adjustments can be processed (e.g. four weeks, or a small number of immediate past periods). If the employee is an Auto employee whose pay is built by Aurion automatically then adjustments made to past periods will be automatically adjusted **M58:** *Approval of prior period adjustments prior to processing.* When a prior period adjustment is required, the details are documented on a standard form requiring approval from an appropriate authority prior to processing. The adjustment is then processed in the system by a member of the payroll team. Report: Trial Pay ER368_PAYRUN. **M59:** *Review prior period adjustments.* On a monthly basis, a report should be generated that lists all prior period adjustments processed. This report should be reviewed to determine the appropriateness of adjustments processed. Report: While there is no standard report within Aurion for prior period adjustments, there is a pay transaction audit report ER016_PAY_AUDIT that produces output detailing all pay transaction audit records that meet the parameter from a range of selection criteria.

IMPORTANT UPDATE

R405: Payroll calculation is inaccurate or incomplete	
Risk type	
Consequence	Draft payroll proposals are not reviewed for reasonableness prior to finalisation of the payroll, resulting in failure to detect significant anomalies or errors.
Better practice	**S22:** *Restrict changes and user access to modify payroll calculation rules.* Personnel calculation rules are used to calculate gross and net pay for employees and should be protected from being overridden or modified without appropriate authorisation. Due to the modular task based nature of the security in Aurion the ability to change underlying payment rules can be restricted to a system administrator or super-user by adding or removing tasks against the appropriate profile (ES651_SECPR_TREE). Changes to an individual's record can be set to require an approval where it is a leave type using the Approval Required field in the time code detail (ES162_TIME_LIST) and changes to work or allowance transactions will always require approval. **M60:** *Review payroll control reports and variance reports.* Useful reports to review prior to finalisation of the payroll include: • Payroll Exception Reports are effective where there is little variation between pay periods. Approved documentation such as leave forms, new engagements, terminations, change in pay rate, and change in deductions should be available to justify the period variation; • Payroll Budget to Variance Reports are effective in identifying significant differences; and • Employee Changes Reports highlight new employees, terminated employees and transfers to ensure only current and valid employees are included in the pay run. Once the reviewer is satisfied with the payroll calculation, a final payroll report should be produced and a copy filed. Report: ER271_EXCEP_RPT – This payroll exceptions report provides the ability to report on a wide range of payroll related conditions, and for which no complex parameter settings, calculations or comparisons are required.

IMPORTANT UPDATE

R406: Statutory obligations for payment of taxation are breached	
Risk type	
Consequence	ATO requirements including PAYG and FBT payment requirements, are breached through failure to retain adequate records or report on and remit tax by specified deadlines, potentially resulting in penalties or reputational consequences.
Better practice	**S23:** *Restricted access to establish and amend taxation reference tables.* The ability to upload and amend tax tables within the HRMIS should be restricted and changes to reference data should be approved prior to the change being implemented. Access to upload or amend tax tables (ES312_TAX_RATES) can be secured via normal task/profile_ security. **M61:** *Review and approval of Fringe Benefits Tax return by appropriate authority.* The amount of FBT payable is self-assessed by the entity. Prior to lodgement of the annual FBT return, detailed review should be undertaken by an appropriate person to determine whether: • Confirmation that a fringe benefit which has been provided is accurate; and • Where a fringe benefit has been provided, the applicable rates and thresholds have been accurately applied in the calculation outlined within the return.

R407: Breach of legislative requirements relating to superannuation	
Risk type	
Consequence	Insufficient superannuation is paid, or payment is not made prior to the quarterly cut-off date. ATO guidance is contravened due to failure to retain adequate documentation in support of super contributions.
Better practice	**S24:** *Configure automated calculation of superannuation payable.* Flagging employees as eligible or ineligible for super contributions and setting the percentage of super payable should enable the super amount payable per period to be automatically calculated by referencing the payroll calculations (for salaries and wages paid) and relevant master data, such as salary sacrifice amounts and additional employee contributions. Superannuation payments are configurable and can be set to pay a percentage of gross pay or annual salary or a fixed amount. This in turn can be deducted from the employee's gross or net pay or as an employer cost. Up to 6 combinations of the above can be configured for a single employee but if required multiple super funds can be set for a single employee. The funds are defined using the Superannuation Funds (ES425_FUND_LIST) task.

IMPORTANT UPDATE

R408: Salary sacrifice arrangements are not appropriately managed	
Risk type	
Consequence	Salary sacrifice arrangements are not clearly documented and the components are not captured in the HRMIS, leading to inaccurate taxation calculations, payments, and disbursements. Non-allowable items are included as part of a salary sacrifice arrangement. This may lead to inaccurate fringe benefits and PAYG tax calculations.
Better practice	**S25:** *Salary sacrifice details are appropriately established in the HRMIS.* The ability to establish and amend salary sacrifice details in the HRMIS should be restricted to appropriate roles within the entity, having regard to enforcing effective segregation of duty controls. In addition to the ability to restrict users from making payroll changes the system allows for individual payment and deduction types, such as salary sacrifice deductions, to be secured separately. This is achieved by creating a new Security type task from Tasks (ES002_TASK_LIST) and recording this new task in the Security Task field of the Time, Allowance or Deduction code. **M62:** *Review and monitor changes to key salary sacrifice information.* Set-up of the salary package elements and rules should be independently reviewed to ensure the following: • Configuration accurately reflects the documented salary sacrifice agreement; • The salary/wage component has been accurately captured to enable accurate PAYG withholding; • Sacrifices which constitute fringe benefits have been accurately classified and captured to enable accurate Fringe Benefits Tax self-assessment; • Sacrificed superannuation is set up as an employer contribution (to be subject to taxes associated with this type of contribution) effective 1 July 2009; and • Salary package elements outside the policy framework are not included as part of the arrangement.

R409: Methodology for performance payment is not established	
Risk type	
Consequence	Unauthorised or inaccurate bonus payments may be disbursed to employees. Bonuses may not be adequately accounted for throughout the period.
Better practice	**S26:** *Utilise system functionality to accrue for and calculate bonus payments.* Where bonus payments are based on a percentage of employee base salary or can be calculated using data established in the system, the automated accrual and payment calculation should be utilised to reduce the risk of inaccurate accrual and calculation. Where automatically calculated, the system output should be independently reviewed by an authorised HR representative for accuracy. Aurion can have a percentage or rate allowances configured to enable a calculation based on an amount paid by specific transactions. Aurion has the flexibility to enable configuration that will allow certain accruals based on whatever trigger that is required. Allowances are configured via the Allowance Code (ES236_ALLW_LIST) task and accruals via the Return Based Accruals section of the Leave Entitlement screen within each Leave Type.

IMPORTANT UPDATE

R410: Employee benefits are not managed or administered in accordance with employee agreements	
Risk type	
Consequence	Employees may receive benefits to which they are not entitled, potentially resulting in financial loss to the entity. Entity may breach terms of enterprise agreements through poor management of employee benefits process.
Better practice	**S27:** *Correctly establish and manage employee benefits.* Eligibility for employee benefits should be established by pay structure/employee role/employee type. When adding a participant, the system should be configured automatically to reference the position (if eligibility is based on level in the organisation) and should prevent participation of ineligible employees or employee classifications. If eligibility is based on information contained in master data (for example, years of service), master data should be automatically referenced to block participation of ineligible employees. In Aurion a Base Salary is set up to calculate an employee's salary and the employee's Allowances, Deductions, Superannuation, Salary Sacrifice, Tax variations, that enables the building of an employee's total benefits. **S28:** *Restricted access to establish benefit plans.* Access to establish benefit plans, enrol employees, create employee specific information associated with the plan and amend plan or employee information should be restricted to appropriately authorised personnel. Aurion can restrict access to all areas of the system based on the Security profile and menus provided to users. See R202 for detailed information.

IMPORTANT UPDATE

8.4 Aurion controls for system maintenance and integration

The control considerations in managing and maintaining Aurion should be consistent with control considerations for other key business systems of the agency. Specific control elements which should be given additional consideration would include change management and interface management. Owing to the complexity and potential confidentiality considerations arising from changes made within the HRMIS context, additional consideration should be given to checking that changes made to employee data and payroll configuration values are in line with approved changes. Interface management controls over internal and external system interfaces between the HRMIS should have appropriate controls to safeguard the sensitive information from a confidentiality and completeness perspective.

The management of integration between the payroll module and the General Ledger is a critical control consideration within an Aurion environment. It is important that payroll-related General Ledger accounts are established correctly and the integration settings are correct. Interface controls including reconciliation and error handling processes must be implemented to the General Ledger system.

Key control objectives

Control objective	Risks mitigated
Payroll information is completely and accurately posted to the General Ledger via the payroll journal.	**R501:** Payroll system does not reconcile to the General Ledger.
Information regarding superannuation contributions is submitted to superannuation funds (such as ComSuper) via an automated interface, ensuring complete and accurate transfer of data.	**R502:** Incomplete or inaccurate submission of superannuation data.
The rate at which leave accrues and leave types to which employees are entitled is accurately established.	**R503:** Leave accrual rates are established inaccurately.
Fields requiring translation into a foreign currency correctly reference accurate foreign exchange rates within the HRMIS to enable accurate calculations.	**R504:** Employee wages paid in foreign currency are calculated incorrectly.
The organisational chart within the application is continuously maintained to accurately reflect vacant and filled positions within the entity, assisting with position management and recruiting efforts.	**R505:** The HR system organisational chart does not accurately reflect current employees and their position.
Payroll schemas and business processing rules are comprehensively and accurately established to enable a stable payroll calculation requiring minimal manual intervention, and are protected from unauthorised modification.	**R506:** Payroll schemas established or modified inaccurately or without authorisation.
Risks to business systems are generally reduced when available patches are installed in a timely manner after being tested for reliability and usability.	**R507:** Application is vulnerable to security or availability threats.

IMPORTANT UPDATE

Risks and controls

R501: Payroll system does not reconcile to the General Ledger	
Risk type	
Consequence	The payroll system should reconcile to the General Ledger to ensure integrity of the financial statements. If not reconciled, or reconciled incorrectly, there is an increased risk of material misstatement in the financial statements.
Better practice	**S29:** *Utilise auto-posting functionality.* Where auto-posting functionality is available within the application, it should be utilised to update the General Ledger. Appropriate configuration between the systems is required, and this should be manually triggered so that only final approved payroll results are updated to the General Ledger. Aurion is an open database which means it works with multiple FMIS systems, Aurion is configured to fit in with whichever FMIS the client is using. Aurion creates posting lines automatically based on information stored against the payment type and establishment data. The posting lines can be generated multiple times to allow for checking of data and then locked when final amendments are made. Posting lines are generated by running the Generate Liab & Expense Adjs (EV724_LVCOST_DRV), Generate On Costs (EV657_ONCOST_DRV) and Costing Analysis (EV579_COSTBK_DRV) tasks. The output file for the FMIS is generally created via the Generic Journal Export (EV131_JOURNAL) although this is not the case for all users. **M63:** *Review of payroll posting results.* A review of payroll results that have not posted to the General Ledger should be performed at each pay cycle. If payroll transactions are manually posted (or a file manually uploaded into the General Ledger), a reconciliation should be performed and payroll that is not posted should be actioned.

R502: Incomplete or inaccurate submission of superannuation data	
Risk type	
Consequence	Information submitted to the superannuation fund is incomplete or inaccurate, potentially leading to penalty payments or incorrect reporting of superannuation payments.
Better practice	**S30:** *Superannuation data is provided in the required format and in the required timeframes.* Superannuation data should be provided in the required format and in the required timeframes as defined by the relevant recipient. Where available, the entity should generate such reports and data from the payroll system data. Superannuation data is exported in the required format for most funds (e.g. PIF, ClikSuper) via Aurion created tasks. As there are too many standard outputs to list in this document please contact Aurion Corp for details on any specific interface. Where a funds requirement is not currently supported it is possible to use the internal Aurion Query Tool (ES328_QUERY_MGR) to create an export file.

IMPORTANT UPDATE

R502: Incomplete or inaccurate submission of superannuation data	
	S31: *Changes to superannuation interfaces and data file formats are managed using entity IT change management controls.* Changes and upgrades to the HRMIS should not inadvertently modify customised interfaces or data files. No modification to standard Aurion outputs are possible via software configuration. Aurion can produce report outputs as PDF documents to further reduce this risk.

R503: Leave accrual rates are established inaccurately	
Risk type	$
Consequence	Inaccuracies in leave accruals reduce the accuracy and reliability of the payroll calculation and associated financial reports.
Better practice	**S32:** *Manage leave accrual rules.* Leave accrual rules are used to calculate employee leave accruals. The leave accrual rules should be consistent with employee conditions for employment (and/or employee agreement) and linked within the application to employee entitlement information. Leave accrual rules are configurable and it is possible to have any number of different award types with different accruals in each. Accruals can be based on a regular accrual amount or varied on the amount of work or other hours paid. Accruals are defined in the Leave Entitlements section of each Leave Type (ES159_ALVE_LIST). **S33:** *Configuration of maximum values for leave accruals.* If employee conditions of employment specify a maximum amount of leave which can be accrued or carried forward, maximum values should be configured for each type of leave accrual. If the maximum leave accrual amount is reached, an error message should be reported and the system designed to stop accruing further leave. Report: ER111_LEAVE_BALS – This report displays balances for leave types that have balances, for all nominated employees. The report includes the pro rata calculated balance in hours and days, and is the balance as at the start of business on the report date. **M64:** *Regular review of employees' leave accruals should be performed.* A manual review of employee's leave accruals should be performed by managers to assess for reasonableness against known periods of leave taken by employees. A further review should be performed by HR to identify any excessive or negative balances.

R504: Employee wages paid in foreign currency are calculated incorrectly	
Risk type	
Consequence	Use of inaccurate foreign exchange rates for currency translation purposes will result in inaccurate calculation of payroll.
Better practice	**S34:** *Establish automated updates for foreign exchange rates.* An automated update of foreign exchange rates should be established with an authorised source and the entity application to ensure rates applied are up to date and accurate. Organisations may pay overseas employees in a single currency based on the Posting Country location. For the duration of a posting, all allowances and salary are paid in the same local currency.

R505: The HR system organisational chart does not accurately reflect current employees and their positions	
Risk type	
Consequence	Incomplete organisation chart may impair the accuracy of workflows associated with self-service functionality, and user access privileges. Other impairments include headcount errors and incorrect workforce planning decisions.
Better practice	**S35:** *Restricted access to update organisational chart.* Access to update the organisational chart should be restricted to appropriate personnel. Amendments should only be processed based on appropriately approved documentation (for example, authority to create a new position). Access to amend establishment information is controlled via the use of security tasks within profiles. See R202 for details. Recording the details of the reason for the amendment can be made mandatory for all establishment changes via Business Rule 01304. **S36:** *Ability to display temporary assignments.* Functionality enabling the organisational chart to display temporary assignments should be utilised to enable tracking of higher duties assignments. Aurion has a temporary assignment (acting placement) recording mechanism. This controls payment of any additional monies as well as flowing through the changes to organisational and other reporting. Acting Placements are recorded using Add Acting Placements (ADD_NON_SUBSTANT) although there are several other ways to enter this information including from Employee Self Service and the Payroll Workbench. **S37:** *Organisational chart designed to reflect the hierarchy.* The organisational chart should be designed to reflect the hierarchy for each department or organisational unit. Aurion can utilise 3rd party organisational charting tools to provide visual representation of positional reporting structures but is able to display organisational reporting structures natively via the Organisation Workbench (ORG_WORKBENCH). Positional reporting structures are recorded in Aurion and used for workflow of leave & timesheet approvals and so on. The Functional Reports To Position field within each position record is used for this purpose.

R506: Payroll schemas established or modified inaccurately or without authorisation	
Risk type	
Consequence	Payroll accuracy is impacted as a result of errors caused by the incorrect set-up of payroll schemas or rules that cause the schemas to execute calculations inaccurately.
Better practice	**S38:** *Access to establish or modify payroll schemas or elements and rules is restricted.* Access to set up or modify payroll schemas or elements and rules should be restricted to appropriate personnel. Access to establish or modify payroll schemas can be secured via task security. See R202 for detailed information.

R507: Application is vulnerable to security and availability threats	
Risk type	
Consequence	A software update is not installed in a timely manner or not installed completely and accurately, making the application vulnerable to security breaches and threatening the availability of the application.
Better practice	**S39:** *Automatic notification of available software updates.* Automatic notification should be configured to alert the system administrator whenever a software update is available. Notification of available software updates is controlled via an administrative function rather than coded into the software itself. **M65:** *Timely installation of approved software updates.* All software updates should be tested in a controlled environment (replicating the production environment) before being released into production.

IMPORTANT UPDATE

8.5 Useful reports for Aurion Human Resources and Payroll Management

The *Aurion Human Resources and Payroll Management module* provides standard reporting functionality. The table below provides a list of specific reports to the HR functions that are useful tools for both management decision making and internal controls. The list does not include customised reports which will be different for each agency.

Code	Name	Description
HR and payroll data management		
ER539_AUDIT_EXP	Audit Output Enquiry	Enables provision of a selection of audit records that can be output to a file and then used as input to a desktop application for further analysis.
ER016_PAY_AUDIT	Pay Transaction Audit Report	Produces output detailing all pay transaction audit records that meet the parameters selected from various selection criteria.
ER023_DELLVE_RPT	Deleted Leave Occurrence Report	Lists deleted leave occurrences
ES842_LVE_LIST	Leave Occurrence Enquiry	Is used to view or enquire on all leave occurrences recorded in Aurion.
ER949_LVE_LIMIT	Excess Leave Balances Cull/Transfer/Warn	This function provides the capability to process excess leave balances for employees. The excess balances can be culled, transferred, paid out or just noted on the employee's payslip
ER148_ACCNT_SUM	Account Posting Summary Report	Lists, for a selected account, the posting rules, costing overrides and offset account details. It does not, however, include the additional rules from the Account Switching form.
ER432_MST_SNAP	Master File Changes & Snapshot Report	Provides information on entitlement and master file changes from one pay run to the next. The report provides a snapshot of all entitlements, as displayed on the Payroll Workbench Benefits Form.
ER150_DUP_EMP	Duplicate Employee Report	Lists groups of employees that have similar details to another employee.
Employee commencement		
EV178_EMP_SHOT	Employee Output Enquiry Report	This function provides a facility where details of employee placement, leave, people and training information are collected.
ER091_PROFILE_RP	Employee Profile Report	Provides a complete profile of the employees in an organisation and produces a series of separate reports relating to the selected reporting options.
Position management		
EV173_POSN_HIER	Position Hierarchy Report	Produces a comma-delimited output file of position details and occupancy for the selected position and all its subordinate positions.

IMPORTANT UPDATE

Code	Name	Description
ER026_CLASS_RPT	Classification Report	Displays details of each classification recorded in Aurion.
ER024_CLASS_VAL	Classification Validation Report	Should be run after adding or modifying classification records. The report displays details of each classification recorded in Aurion and runs a series of checks against every classification and related increment.
ER092_PROF_SALHS	Employee Salary History Report	Provides a summary of an employee's placements and acting placements, detailing either the annual or fortnightly salary amount for the placement.
ER076_ORG_STAFF	Organisation and Staff Report	Provides a summary of organisation units, positions, placements, actual placements and, if required, unattached staff.
ER008_IN_OUT	Staff Movement Report 1	Lists staff movements in and out of a specified organisation unit and reports by Movement Type and Classification for a specified period.
EV366_STF_MV_RPT	Staff Movement Report 2	This customer-specific report produces a comma delimited text output file on placement movements within an organisation unit range and a user defined date range. The report identifies movements into, within, and out of the selected organisation unit range.
ER010_STAF_UNATT	Unattached Staff Report	Lists, by organisation unit, those staff whose current actual placement does not have a position number.
EV366_STF_MV_RPT	Placement Changes Report	This customer-specific report provides aggregated data of staff movement and headcount for each department selected on the parameter form, within a specified date range.
ER029_OUSEC_RPT	Organisation and Position Security	Lists Organisation Units and Positions and, for each Organisation Unit and Position, provides details of the respective Organisation Unit Profile, Organisation Unit Access, Position Profile, and Position Access.
Employee exits and terminations		
EV551_PAYSUMHST	Pay Summary History Report	This customer-specific report provides a summary of employee pay details based on the employees' position within the organisation structure within the nominated historical reporting period. Employees included in this report may currently be terminated and included in the report where the report is run retrospectively and the employee used to be in the reported organisation unit (range) on the 'report as at date'.

Code	Name	Description
Time reporting		
ER090_MAN_CONT	Management Control Report	Details the hours and amounts processed for employees in a nominated pay entity or organisation unit within specified date range.
Payroll processing and administration		
ER111_LEAVE_BALS	Leave Balances Report	Displays balances for leave types that have balances, for all nominated employees. The report includes the pro rata calculated balance in hours and days, and is the balance as at the start of business on the report date.
EV523_LVE_ENQIRY	Leave Output Enquiry Report	Details the occurrence of employee leave, placements, people and employment information.
ER020_LVE_LIABIL	Leave Liability Report	Conforms to the requirements of AASB 1028 Accounting for Employee Entitlements. The report shows the number of hours leave and the dollar value of leave entitlements by person and organisation unit based on actual placements.
ER018_LVE_OCCUR	Leave Occurrence Report	Is an on-line leave enquiry facility allowing you to report by employee or organisation unit. It provides information such as which employees are currently on leave, the type of leave and the cost and duration of the leave.
ER070_COST_BREAK	Costed Breakdown Report	Provides breakdown details for each payroll transaction and includes pay entity details, pay record details, transaction details, costing information details and dollar breakdown allocation amounts.
EV521_HRB_COST	Costing Output Enquiry Report	Provides details of employee's costing breakdown, pay and employment information. You can report by one or more pay agencies, or by organisation unit, and specify the pay period to report on.
ES892_EALLW_LIST	Allowance Transactions Enquiry	This function is used to view and enquire on all allowance transactions recorded in Aurion.
ER019_PAY_SUM	Pay Summary Report	Is designed to report on a variety of selected pay summaries made across a range of pay periods or in a single pay period. The output can be presented in summary or detail form.
ER271_EXCEP_RPT	Payroll Exceptions Report	Provides you with the ability to report on a wide range of payroll related conditions, and for which no complex parameter settings, calculations or comparisons are required.
ER112_PAY_EXCEPT	Payroll Reconciliation Report	Checks that the payroll can be reconciled. It performs various checks and reports the results.

IMPORTANT UPDATE

Code	Name	Description
ER062_PAYROL_TAX	Payroll Tax Report	Summarises gross payroll item amounts by their payroll tax category. This results in summarising payroll item amounts that attract different rates of payroll tax and those that attract no payroll tax.
ER039_YTD	Person Year To Date Report	Provides a combination of pay summary and pay transaction totals for a specified financial year or a specified date range.
EV370_T_SAL_RPT	Total Salary Report	This customer-specific report provides details of placement salary, standing allowances, standing employer deduction benefits, and employer superannuation into discrete hourly rate and annual value columns for each employee reported.
ER200_TXVAR_RPT	Transaction Variance Report	Allows you to nominate a range of payroll transaction scenarios on which to report. The report has two primary functions: Compare transaction totals with the SAME transactions from the Previous Period Compare transaction totals with DIFFERENT transactions from the SAME Period

IMPORTANT UPDATE

IMPORTANT UPDATE

Human Resources Management Information Systems – Risk and Controls

Better Practice Guide

Appendices

IMPORTANT UPDATE

IMPORTANT UPDATE

Appendix 1: HR information and good privacy practice

During each stage of the employment lifecycle—before, during and after employment—agencies will collect personal information. This means that it is very important that agencies have in place systems to collect and manage this information in a way that complies with all legal and policy requirements. Australian Government agencies are required to comply with the eleven ***Information Privacy Principles*** under section 14 of the *Privacy Act 1988 (Cth)*.

Agencies that elect to outsource their HR functions to a private sector organisation should ensure that an additional set of principles, the ***National Privacy Principles***,[19] apply to the service provider—therefore the provider will need to comply with both the Information Privacy Principles and the National Privacy Principles. Further detail is available in an information sheet: *Privacy Obligations for Commonwealth Contracts* and is available from the Office of the Australian Information Commissioner (OAIC).

This article highlights better practice considerations for Australian Government agencies in order to reduce the risk of non-compliance with these key legislative requirements.

Separate guidance and more detail on the Information Privacy Principles and the National Privacy Principles is set out on the Commissioner's website: http://www.oaic.gov.au

Information Privacy Principles

A summary of the 11 Information Privacy Principles (IPP) is outlined in the diagram below:

IPP 1	Manner and purpose of collection of personal information
IPP 2	Solicitation of personal information from individual concerned
IPP 3	Solicitation of personal information generally
IPP 4	Storage and security of personal information
IPP 5	Information relating to records kept by record-keeper
IPP 6	Access to records containing personal information
IPP 7	Alteration of records containing personal information
IPP 8	Record-keeper to check accuracy of personal information before use
IPP 9	Personal information to be used only for relevant purposes
IPP 10	Limits on use of personal information
IPP 11	Limits on disclosure of personal information

Appendices

19 From 12 March 2014, the *Australian Privacy Principles* will replace the *National Privacy Principles* and *Information Privacy Principles* and will apply to organisations, and Australian, ACT and Norfolk Island Government agencies.

IMPORTANT UPDATE

Personal information includes any information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. Where information is stored in a personnel file, the entire content of the file is likely to be personal information as it directly relates to the individual. Section 6 of the Privacy Act 1988 provides a full definition of personal information.

IPP 1: Manner and purpose of collection of personal information

Information Privacy Principle 1 prohibits agencies from collecting personal information for inclusion in a record or a generally available publication unless the:

- information is collected for a purpose that is a lawful purpose directly related to a function or activity of [the agency]; and
- collection of the information is necessary for or directly related to that purpose.

In addition, the information should not be collected by unlawful or unfair means. The nature of human resources and payroll processes means that collection of personal information—including tax file numbers and bank details—is a necessity. Particular care needs to be taken in relation to information requested for pre-employment security or health checks as this will usually involve very sensitive information.

Better practice considerations

Personnel involved in HR functions that legitimately require the collection of personal information are aware of the manner in which information should be collected.	Training should be provided to HR and payroll personnel to ensure they are aware of what constitutes unlawful or unfair means to collect information.
There is an clear link between the information collected, and the purpose for collecting that information.	Each entity should document a policy clearly stipulating the purpose for collection of personal information at all stages of the employment process.

IPP 2: Solicitation of personal information from individual concerned

Information Privacy Principle 2 requires the agency to clearly inform the individual from whom the information is being collected:

- the purpose for which the information is being collected;
- if that information is being collected as required by or under law and, if so, what that law is; and
- any person or body to whom the information is usually disclosed.

The collector must inform the individual prior to collection of the personal information, or as soon as practicable after collection. This principle applies no matter how information is requested. For example, agencies will be collecting information as part of their recruitment processes if individuals:

- complete an online self-assessment;
- provide hardcopy or electronic information with their applications;
- answer questions at the interview; or
- provide further information as part of pre-engagement security checks.

This means that it is important that agencies:

- assess what information is being requested at each stage of the employment cycle;
- assess what purposes the agency will use that information for;
- assess what other agencies or third parties the information may be disclosed to; and
- notify individuals about those purposes and potential disclosure at the point of collection.

Better practice considerations

The individual should be informed of the purpose for collection of information and the authorisation for the collection.	Use of a standard information sheet be provided to individuals (for example, job applicants) from whom common personal information is required. This information should also be readily available to personnel involved in recruitment processes

IPP 3: Solicitation of personal information generally

Information Privacy Principle 3 builds on the requirements for collection of information under Information Privacy Principle 1. It requires that agencies take steps to provide that the information collected is:

- relevant to the purpose for which it is collected; and
- up-to-date and complete.

It also emphasises that collection of the information should not "intrude to an unreasonable extent upon the personal affairs of the individual concerned."

At each stage of the employment cycle it will be necessary to collect some personal information. The purpose of much of that information will be clear. For example, agencies will need to collect bank account information from employees in order to pay them.

There may still be some information where judgement is required as to whether or not it is 'unreasonable' to collect the information. For example, agencies should be cautious when using applicant testing procedures. These tests should only ask job-related questions and not ask overly intrusive questions.

It is also important for agencies to consider where information is being obtained from as part of their obligation to collect information that is accurate and up-to-date. This means that generally it is better practice to collect information from the individual concerned, unless this is not possible in the circumstances (for example, in the case of referee checks).

Better practice considerations

Information collected should not be unreasonably intrusive and should be relevant, up to date and complete	Policies on lawful and reasonable questioning of job applicants are developed and communicated to relevant employees.

IPP 4: Storage and security of personal information

Information Privacy Principle 4 requires that agencies make certain that records containing personal information are "protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse."

This principle relates to information stored both in IT systems and in hard copy. This means that agencies' HR systems and procedures include the following:

- backup controls are put in place, including regular backup of information and off-site storage of backup tapes;
- hard copy information is stored in locked fireproof cabinets;
- access to buildings and rooms in which information is stored is appropriately restricted;
- access to information systems (including backup systems) in which information is stored is appropriately restricted based on job requirements;
- access to underlying data (such as employee files) is appropriately restricted; and
- identity verification checks are undertaken prior to releasing personal information to the individual, or other authorised officers.

In addition, where the collector is required to provide information to another person or entity, reasonable steps should be taken so that the third party does not disclose the contents of the information. This could include simply informing the person or entity of the confidential nature of the information (which is generally adequate for government personnel or agencies), or requesting that the person or entity signs a non-disclosure agreement prior to releasing the information.

Particular care should be taken when any part of the HR function is outsourced to ensure that the agency has done "everything reasonably within [its power] … to prevent unauthorised use or disclosure of information [contained within employee records]."

Better practice considerations

Security safeguards are implemented to protect personal information against loss, unauthorised access, use modification, disclosure, and misuse.	Implementation of information system controls are sufficient to safeguard information stored by the agency.

System considerations

Payroll master data is an area of high-risk in terms of fraud or overpayments. Accordingly, user access to perform functions such as amending or updating master data should be restricted, with access being provided in line with job requirements. Users that have access to amend or update master data should not have the ability to perform payroll functions. Periodic review of this data is an important control, such as review of a master data change report. Changes to master data should be periodically checked against the source documentation that requested and authorised the amendment.

IPP 5: Information relating to records kept by record-keeper

Information Privacy Principle 5 relates to the systems that agencies have in place to ascertain and disclose the type of personal information they hold. Agencies must maintain a 'master' record that sets out the:

- nature of the records of personal information kept by or on behalf of the [agency] (i.e. the type of personal information stored);
- purpose for which each type of record is kept;
- classes of individuals about whom records are kept;
- period for which each type of record is kept;
- persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and
- steps that should be taken by persons wishing to obtain access to that information.

This 'master record' should not itself contain any personal information as it must be:

- made available for public inspection; and
- provided to the Privacy Commissioner every year in June.

Usually agencies will appoint a privacy officer who coordinates the submission of these records on a whole of agency basis.

Better practice considerations

Agencies are aware of the type and nature of the information they are collecting and retaining.	Data management policies stipulate information that is required to be maintained.

System considerations

Systems should be configured to require entry of the above information before a new listing of records can be created.

IMPORTANT UPDATE

IPP 6: Access to records containing personal information

Information Privacy Principle 6 allows individuals to access any records that contain personal information about them "except to the extent that the [agency] is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents".

This principle allows an individual about whom personal information has been collected to have access to that information, unless restricted under another law. This right to access is separate from the freedom of information process. IPP 6 provides the same right of access to information as is available under the *Freedom of Information Act 1982 (Cth)*, but the *FOI Act* contains different review and appeal provisions. For example, under the *FOI Act* an agency must release requested documents unless they fall within certain exemption categories, and under current reforms to the *FOI Act*, there is no charge for access to personal information.

A particular application of this in the HR context is that an agency employee may ask to view their own personnel file at any time. Similarly, job applicants may also ask to view notes made about them, or reasons documented for their lack of success in securing a role.

It is important for information to be maintained and disposed of in accordance with relevant legislation and agencies should confirm record-keeping obligations before disposing of information. Data cleansing activities should be undertaken in accordance with the requirements to retain Commonwealth Records under the *Archives Act 1983 (Cth)*, and records should only be disposed of in accordance with a disposal authority.

Better practice considerations

Information is maintained in accordance with legislation.	Information should be periodically reviewed and disposed of, where no longer required, in accordance with relevant disposal authorities.

IPP 7: Alteration of records containing personal information

Information Privacy Principle 7 requires agencies to take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that their records of personal information:

- are accurate; and
- has regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

Employee self-service facilities allow for the modification of many items of personal information by employees in a way that enables these records to be maintained accurately and in a timely manner. This does not remove agencies' responsibilities for ensuring that records are up-to-date. Where an individual requests a change to their personnel file, if the change is not made this also needs to be noted on their personnel file, including the reasons for not making the change. Accordingly agencies procedures and systems should have the facility to do this.

Better practice considerations

Updates to payroll or HR master data are inaccurate or are processed appropriately authorised.	Perform reconciliation between data recorded in the HRMIS at a point in time to authorised documentation to ensure the change was made accurately.

IPP 8: Record-keeper to check accuracy of personal information before use

Information Privacy Principle 8 requires agencies not to use personal information "without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete."

Information Privacy Principle 8 builds on Information Privacy Principle 7 by requiring the agency to take reasonable steps prior to using information to ensure that it is accurate, up to date and complete. Consideration should be given to requesting that personnel confirm details that may be out of date (either on a periodic basis or prior to use of information).

IPP 9: Personal information to be used only for relevant purposes

Information Privacy Principle 9 requires that an agency "who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant." In other words, agencies should only use personal information for a purpose to which it is relevant.

To assist with complying with this IPP, it is suggested that agencies develop a clear policy on use of personal information, and provide training to relevant personnel concerning the appropriate use of information.

IPP 10: Limits on use of personal information

Information Privacy Principle 10 applies in addition to Information Privacy Principle 9. This means that information can only be used for a purpose if:

- it is relevant to that purpose (IPP 9); and
- either it was collected for that purpose or one of the exemptions apply (IPP 10).

The exemptions under Information Privacy Principle 10 are:

(a) the individual concerned has consented to use of the information for that other purpose;

(b) the agency believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

(c) use of the information for that other purpose is required or authorised by or under law;

(d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

(e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

There are also exceptions in other circumstances, such as enforcement of criminal law, imposing a pecuniary penalty, or the protection of public revenue.

IPP 11: Limits on disclosure of personal information

Principle 11 restricts the disclosure of personal information, which includes disclosure to other agencies. Agencies must not disclose personal information unless:

- the individual concerned is reasonably likely to have been aware, or made aware under Information Privacy Principle 2, that information of that kind is usually passed to that person, body or agency;
- the individual concerned has consented to the disclosure;
- the [agency] believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
- the disclosure is required or authorised by or under law; or
- the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

Information Privacy Principles under section 14 of the *Privacy Act 1988*

Principle 1

Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
   (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
   (b) the collection of the information is necessary for or directly related to that purpose.
2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2

Solicitation of personal information from individual concerned

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(a) the purpose for which the information is being collected;

(b) if the collection of the information is authorised or required by or under law, the fact that the collection of the information is so authorised or required; and

(c) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first mentioned person, body or agency to pass on that information.

Principle 3

Solicitation of personal information generally

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

IMPORTANT UPDATE

Principle 4

Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5

Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

   (a) whether the record-keeper has possession or control of any records that contain personal information; and

   (b) if the record-keeper has possession or control of a record that contains such information:

      i. the nature of that information;

      ii. the main purposes for which that information is used; and

      iii. the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:

   (a) the nature of the records of personal information kept by or on behalf of the record-keeper;

   (b) the purpose for which each type of record is kept;

   (c) the classes of individuals about whom records are kept;

   (d) the period for which each type of record is kept;

   (e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and

   (f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:

   (a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

   (b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

IMPORTANT UPDATE

Principle 6

Access to records containing personal information

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

Principle 7

Alteration of records containing personal information

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:
   (a) is accurate; and
   (b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.
2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.
3. Where:
   (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and
   (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8

Record-keeper to check accuracy etc of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9

Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

IMPORTANT UPDATE

Principle 10

Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:
   - (a) the individual concerned has consented to use of the information for that other purpose;
   - (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
   - (c) use of the information for that other purpose is required or authorised by or under law;
   - (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
   - (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.
2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Principle 11

Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless the:
   - (a) individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
   - (b) individual concerned has consented to the disclosure;
   - (c) record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
   - (d) disclosure is required or authorised by or under law; or
   - (e) disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.
2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.
3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

IMPORTANT UPDATE

Appendix 2: Implementing self-service functionality

Self-service applications are becoming a primary method to control costs and deliver HR services. These applications provide a web-based interface for employees to perform certain transactions without the need to interact with the HR area. The key benefits derived from self-service applications are increases in service availability and quality, and a decrease in costs and completion time of transactions.

Through self-service functionality, employees can:

- update their personal and banking details;
- apply for leave and other benefits;
- view pay-slips online; and
- view internal job vacancies.

These self-service applications typically include functionality for managers, such as:

- approve timesheets, leave requests and expense claims;
- make corrections to clock in/out entries submitted by an employee;
- initiate personnel change requests such as promotions, salary increases, transfers and terminations; and
- access to employee information such as phone list or employee profile.

A key benefit of the self-service implementation is that as routine administrative services are performed almost immediately without direct HR intervention, the HR function can focus on other operational matters rather than processing activities. However, implementing a self-service solution, such as Employee Self Service (ESS), requires a carefully planned change management process, not only for the HR function, but also for employees and managers.

Consideration of the following steps is important to the implementation and operation of a self-service process:

- determine efficiencies to be gained;
- provide adequate training to employees;
- educate employees and managers on the individual benefits;
- establish an approval process for changes to employee files;
- implement a change management process; and
- develop and implement information security requirements.

Determining efficiencies to be gained

The business case for introducing self-service functionality should clearly describe the cost and benefits, and identify any anticipated impacts to current processes.

In conjunction with preparing the cost and benefit analysis, current corporate and HR strategies should also be reviewed to determine the extent to which self-service will align with these strategies. There are many situations when a self-service solution may not provide benefits or cost savings as intended. Self-service functionality provides the opportunity to reduce the completion time for routine transactions. In situations where an entity uses a complex workflow process that, for example, results in regular workflow exceptions directed to the HR function to complete the transaction, it is likely that there will be limited efficiency gains.

Providing adequate training to all employees

One of the primary benefits of implementing a self-service solution is a reduction in service requests passed to the HR section for routine transactions. Implementation of a new process or system may, in the initial implementation stage, lead to confused or unsure users, and this may in turn lead to an increase in calls to support centres.

By providing adequate training to employees during the implementation, calls for support should be minimal and taper off as employees become more familiar with the system. Managers should be provided with appropriate training in the self-service application and understand the implications of their actions in approving or denying employee requests.

Training employees can be accomplished using several methods. Provision of online materials as well as attendance at online guided training sessions assists with educating employees in the features and process of performing transactions on the ESS solution. A “manager kit” containing information on the new processes and support contact details would provide assistance to promptly address any queries.

Educating employees and managers on the individual benefits

A self-service solution will change the way that employees and managers perform HR-related transactions. Employees may raise objections to changing a process that may have had no issues in the past. Similarly, managers may have a negative perception of the process as they may see it as a transfer of administrative tasks.

It is important that employees support the solution. This may be achieved through educating employees and managers in the tangible benefits of using the solution. Employees will soon discover that they can make updates to their details, apply for leave, or gain access to pay slips instantly. Once managers are accustomed to the additional tasks they are required to perform, they will appreciate that they have better control and visibility in managing their staff and allowing them to better coordinate their resources.

Establishing an approval process for changes to employee files

With an ESS solution, employees are able to manage and update their own personal details such as residential address, bank account details, and skills profile. In general, ESS implementations have demonstrated that when an employee manages their own records, the rate of errors is reduced. Often there is a risk that an employee may submit incorrect details accidentally, or inappropriately seek to fraudulently alter another employee’s details (such as bank account details).

The introduction of an approval process for changes to employee information allows HR staff to view the proposed change to validate that it appears correct. The system configuration should maintain a record of changes made to employee details.

Implementing a change management process

Implementation of an ESS solution may involve the introduction of a new IT system as well as process redesigns to work with the new system. Effective coordination is required to properly implement the solution and to minimise the occurrence of problems.

A change management process should be established to manage the various tasks that need to be undertaken, including:

- underlying data may need to be cleansed or imported into the system;
- a communication plan should be maintained to provide stakeholder awareness of the current status of the rollout of the new system;
- user acceptance testing prior to rollout to determine how clear it is to an employee on how to perform a transaction;
- mapping of the entity organisational chart to determine manager relationships and span of control; and
- testing prior to release of system updates to confirm they will work as intended.

Developing and implement information security requirements

ESS solutions enable employees and managers to gain access to key HR information that is highly sensitive and could be used to cause damage to the employee or the entity. Understanding of the implications of providing access to HR information to employees and managers is essential to comply with relevant legislation.

Security policies should be reviewed when releasing the self-service solution. Specific policies that govern length and complexity of passwords, expiry date, sharing of passwords and access control should be reviewed and updated by the IT department. Security of the systems storing the ESS solution should be reviewed and updated as necessary for data integrity and access.

IMPORTANT UPDATE

Appendix 3: Glossary of Terms

Term	Definition
Access control	The process of restricting access to particular HR Management Information System areas, transactions or functions to authorised users.
Audit report	A report used commonly for performing a detective or review control the report will outline activities undertaken within an HR management information system, for example, changes made to employee records. Also known as a control report.
Aurion	A human resource and payroll management information system, created by Aurion Corporation.
Automated control	Refer to System control.
Change management process	A model which outlines how changes to a system or organisation should be implemented in a controlled manner.
Configuration	The act of setting parameters in the system to control the business processes performed. The system must be configured to meet the needs of the entity before it can be used.
Configuration control	Controls which will be automated if the system is configured in a particular way. Refer to Configuration for further information. Also refer to System controls.
Control objectives	Control objectives are high-level statements by management that provide a link between organisational risks and the internal controls and activities implemented by agencies to mitigate such risks.
Controls	Policies, procedures and practices designed to mitigate and reduce the chance of risks being realised.
Cost centre	Organisational unit within a controlling area that represents a defined location of cost incurrence. The definition can be based on: Functional requirements, Allocation criteria, Physical location and Responsibility for costs.
Customisation	Adjusting a particular aspect of the HR Management Information System or creating a custom add-on for the HR Management Information System that addresses the specific needs of the particular entity using the HRMIS.
Data	Representation of facts, concepts or instructions in a formalised manner suitable for communication, interpreting or processing by users or by automatic means.
Database	Systematically organised or structured repository of indexed information (usually as a group of linked data files) that allows easy retrieval, updating, analysis, and output of data. Most computer applications (including antivirus software, spreadsheets, word-processors) are databases at their core.
Default	The configuration settings that are in place upon installation of the HRMIS.
Duplicate employees	An employee who is listed two or more times on the payroll.
Edit access	Access within an HR Management Information System to input, amend or delete data.
Employee contribution	Amounts contributed to superannuation funds in excess of the statutory employer contribution.
Employee Self Service (ESS)	Online facility as a component of the HR Management Information System where an employee can maintain their time sheet, create leave requests, edit personal information, and display their pay slips.
ESS	Refer Employee Self Service.
Field	A particular characteristic of a particular item that can be input/modified by a user.

Appendices

IMPORTANT UPDATE

Term	Definition
Function	A task that an employee performs to accomplish a specific portion of his/her job responsibilities. A function is a grouping of one or more related actions and/or permissions for a specific business area. It is also referred to as a 'transaction group'. An example of a function is Employee Maintenance. This function would include all of the HR Management Information System transactions that can be used to maintain an employee record.
HRMIS	Human Resource Management Information System.
Human Resource Management Information System	The information system that supports an entity's HR function, allowing the entity to automate tasks such as processing employee payments.
ICT	Information and Communication Technology
Integrity	Within this Guide, used in the context of data, that is, data that is complete and accurate.
Interface	Commands, codes, and messages that enable different programs to communicate with each other and the operating system. More broadly, refers to the transfer or sharing of data between separate systems.
Logical access	Refers to user or system access to data files or computer programs.
Manager Self Service	Online facility as a component of the HR Management Information System where a manager can process functions such as approve timesheets, leave requests and expense claims; correct employee timesheet entries; or initiate personnel change requests.
Master data	Master data, is information that is key to the operation of business. The term is not limited to HR data, and the term is often used to describe key business information that may include data about customers, products, employees, materials, suppliers, etc. which often turns out to be non-transactional in nature. Master data is generally used to support transactional processes and operations, but its use is also central to performance to analytics and reporting.
Module	Part of a program that performs a distinct function.
MSS	Manager Self Service.
Oracle PeopleSoft	In the context of this Guide, a Human Resource Information System created by PeopleSoft Inc, which was acquired by Oracle Corporation in 2005. Referred to in this Guide generally, as 'PeopleSoft'.
Parameters	Parameters define the way the HR Management Information System operates, particularly system logon and password maintenance functions.
Software update	Small program (set of computer code) that modifies one or more files within a software package with the purpose of improving performance of the software.
Payroll calculation	The process of performing the periodic calculation of employee costs, calculation of leave accrual balances and updating these amounts in the financial records of an entity.
Payroll exception reporting	Reporting which shows the difference between what was paid in the prior payroll period and what was paid in the current payroll period.
Physical access	Access to areas rather than to an IT system, for example, access to a building, room, filing cabinet, safe.
Position based security	In position based security, roles are allocated to positions rather than individual users (as distinct from user based security). When a user is allocated to a position in HR, they automatically inherit the access that has been assigned to that position.
Prior period adjustment	An adjustment processed to a period which has been closed or finalised for timekeeping or accounting purposes.
Profile	A collection of authorisations which have been grouped together to be allocated to a user (to assign access capabilities).

IMPORTANT UPDATE

Term	Definition
Reconciliation	Item by item examination of two related sets of figures obtained from different sources.
Risk	A combination of the likelihood of an adverse even occurring and the consequence that such an event may have on the entity.
Role	Logical selection of system based functionality that enables a user to perform specific tasks and functions within a system. Permissions to perform certain operations are assigned to a specific role. Members of staff (other than system users) are assigned particular roles and through those role assignments acquire the permissions to perform particular system functions.
SAP	SAP is the main enterprise resource planning software produced by SAP AG. It is an enterprise- wide information system designed to coordinate all the resources, information, and activities needed to complete business processes such as order fulfilment or billing.
Segregation of duties	A primary internal control intended to prevent a single individual from having control over all stages of a process. The objective of segregation of duties is to ensure that different roles are involved in the different stages of a process, specifically initiation, authorisation/approval, recording and settlement/implementation processes.
Segregation of duties conflict	Two functional duties that, if performed by the same user, increase the chances of fraud and/ or error occurring.
Service Level Agreement	Contract between a service provider and a customer detailing the nature, quality, and scope of the service to be provided.
Single sign-on	Single sign-on (SSO) is mechanism whereby a single action of user authentication and authorisation can permit a user to access computers and systems without the need to enter multiple passwords.
SLA	Refer to Service Level Agreement SOD
Refer to Segregation of duties SSO	Refer to Single sign-on
System control	A control performed automatically by an IT system. In order for this control to operate, it may need to be configured within the system.
Table	A structure used within the HR Management Information System to store transaction data, basic commercial data, configuration and system parameters, organisation structure data, and calculation rules.
Test environment	An area within the HR Management Information System where testing of a system change or software update can be undertaken without adversely affecting information stored within the system, that is, separate to normal data storage and processing. Also known as a non production environment.
Transaction codes	Various functions within the HR Management Information System are referred to as transactions. Most functions can be invoked by a transaction code.
Validation check	A check performed by the system based on rules within the system to warn a user of possible data input error; for example, data field can only be input as DD/MM/YYYY, or an error will occur; DD input cannot exceed 31, etc.
View access	Access to view information within the HR management information system. This type of access does not allow for input, deletion or modification of the data within the HR management information system.
Workflow	A utility that can be used to control the time and logical sequence in which work items are processed; for example, workflow can be used to help automate the electronic approval of timesheets, automatically notifying the appropriate user of the need to authorise a timesheet electronically.

IMPORTANT UPDATE

Appendix 4: Summary of HR functions with related risks and controls

Table Appendix 4.1: Summary of HR functions with related risks and controls

HR function and risk	Risk type	System Control	Manual Control
HR and payroll data management			
R201: HR master data is inaccurate.		S01, S02, S03	M50
R202: HR master data is not secure.		(S02), S04	M51
Workforce management			
R301: Non-existent or duplicate employee is added to the payroll.		(S03), S05	M52
R302: Termination payments and balances are inaccurately calculated.		S06, S07, S08	M53
R303: Employee is not deactivated when employment is terminated.		S09, S10, S11	M54
Payroll processing and administration			
Time reporting			
R401: Inaccurate or incomplete entry of employee time data.		S12, S13, S14, S15	M55
R402: Unapproved leave or leave is taken outside of entitlements.		S16, S17, (S37)	M56
R403: Established employee shifts are updated inaccurately.		S18	M57
R404: Time recorded in prior periods is amended inaccurately or without appropriate authority.		S19, S20, S21	M58, M59
Payroll accounting			
R405: Payroll calculation is inaccurate or incomplete.		S22	M60
R406: Statutory obligations for payment of taxation are breached.		S23	M61
R407: Breach of legislative requirements relating to superannuation.		S24	
R408: Salary sacrifice arrangements are not appropriately managed.		S25	M62

IMPORTANT UPDATE

HR function and risk	Risk type	System Control	Manual Control
R409: Methodology for performance payments is not established.		S26	
R410: Employee benefits are not managed or administered in accordance with employee agreements		S27, S28	
System maintenance and integration			
R501: Payroll system does not reconcile to the General Ledger.		S29	M63
R502: Incomplete or inaccurate submission of superannuation data.		S30, S31	
R503: Leave accrual rates are established inaccurately.		S32, S33	M64
R504: Employee wages paid in foreign currency are calculated incorrectly.		S34	
R505: The HR system organisational chart does not accurately reflect current employees and their position.		S35,S36, S37	
R506: Payroll schemas established or modified inaccurately or without authorisation.		S38	
R507: Application is vulnerable to security or availability threats.		S39	M65

Appendices

IMPORTANT UPDATE

Table Appendix 4.2: Summary of System Controls

Ref.	Control description	HR function	Risk Ref.
S01	Define key data entry field	HR and payroll data management	R201
S02	Restricting user access to view, establish and amend master data.	HR and payroll data management	R201
S03	Validation checks on certain fields warn the user that the information is duplicated in another employee record.	HR and payroll data management	R201
S04	Access to HR master data is appropriately configured and managed.	HR and payroll data management	R202
S05	Access to add an employee should be restricted to appropriate individuals and segregated from payroll maintenance.	Employee commencements	R301
S06	Application will warn user if termination date in the past is entered.	Employee exits and terminations	R302
S07	Workflow operates to require independent approval verification of termination date entered.	Employee exits and terminations	R302
S08	Application automatically calculates payments based on master data, termination date entered, and leave entitlements.	Employee exits and terminations	R302
S09	Application automatically changes status of employee to 'terminated' as at termination date entered.	Employee exits and terminations	R303
S10	Application automatically disables terminated employee's access to systems based on termination date entered.	Employee exits and terminations	R303
S11	Application does not allow payment to be disbursed to employees with 'terminated' status.	Employee exits and terminations	R303
S12	Workflow approval of employee time.	Time reporting	R401
S13	System validation of data entered.	Time reporting	R401
S14	Timesheets are locked for editing after submission.	Time reporting	R401
S15	Automated notifications.	Time reporting	R401
S16	Automated checks on leave applications to confirm sufficient entitlement.	Time reporting	R402
S17	Workflow approval of leave requests.	Time reporting	R403
S18	Restrict user access to amend work rosters.	Time reporting	R404
S19	Restrict user access to process prior period adjustment.	Time reporting	R404
S20	Workflow approval of prior period adjustments.	Time reporting	R404
S21	Limit prior period adjustments.	Time reporting	R404
S22	Restrict changes and user access to modify payroll calculation rules.	Payroll processing and administration	R405
S23	Restricted access to establish and amend taxation reference tables.	Payroll processing and administration	R406

IMPORTANT UPDATE

Ref.	Control description	HR function	Risk Ref.
S24	Configure automated calculation of superannuation payable.	Payroll processing and administration	R407
S25	Salary sacrifice details are appropriately established in the HRMIS.	Payroll processing and administration	R408
S26	Utilise system functionality to accrue for and calculate bonus payments.	Payroll processing and administration	R409
S27	Correctly establish and manage employee benefits.	Payroll processing and administration	R410
S28	Restricted access to establish benefit plans.	Payroll processing and administration	R410
S29	Utilise auto-posting functionality.	Managing system interfaces	R501
S30	Superannuation data is provided in the required format and in the required timeframes.	Managing system interfaces	R502
S31	Changes to superannuation interfaces and data file formats are managed using entity IT change management controls.	Managing system interfaces	R502
S32	Manage leave accrual rules.	Managing system rules	R503
S33	Configuration of maximum values for leave accruals.	Managing system rules	R503
S34	Establish automated updates for foreign exchange rates.	Managing system rules	R504
S35	Restricted access to update organisational chart.	Managing system rules	R505
S36	Ability to display temporary assignments.	Managing system rules	R505
S37	Organisational chart designed to reflect the hierarchy.	Managing system rules	R505
S38	Access to establish or modify payroll schemas or elements and rules is restricted.	Managing system rules	R506
S39	Automatic notification of available software updates.	Managing software updates	R507

IMPORTANT UPDATE

Table Appendix 4.3: Summary of Manual Controls

Ref	Control description	HR function	Risk Ref
M50	Establishment and amendment of master data occurs only when supported by appropriately approved documentation.	HR and payroll data management	R201
M51	Review of system configuration reports.	HR and payroll data management	R201
M52	When adding a new employee, a listing of current employees should be reviewed to reduce the risk of duplicating the employee record.	Employee commencements	R301
M53	An independent authority checks the termination date per notification documentation to the date entered in the system.	Employee exits and terminations	R302
M54	Department/Cost Centre Managers are periodically provided with a listing of employees for which they are responsible. This listing is checked to determine whether it contains any employees no longer working within the department.	Employee exits and terminations	R303
M55	Review 'Missing Time' report.	Time reporting	R401
M56	Periodic review over recording of leave.	Time reporting	R403
M57	Approval of updates to work rosters.	Time reporting	R404
M58	Approval of prior period adjustments prior to processing.	Time reporting	R404
M59	Review prior period adjustments.	Time reporting	R404
M60	Review payroll control reports and variance reports.	Payroll processing and administration	R405
M61	Review and approval of Fringe Benefits Tax return by appropriate authority.	Payroll processing and administration	R406
M62	Review and monitor changes to key salary sacrifice information.	Payroll processing and administration	R408
M63	Review of payroll posting results.	Managing system interfaces	R501
M64	Regular review of employees' leave accruals should be performed.	Managing system rules	R503
M65	Timely installation of approved software updates.	Managing software updates	R507

Index

Index

IMPORTANT UPDATE

IMPORTANT UPDATE

www.anao.gov.au

Human Resource Management Information Systems

The *Financial Management and Accountability Act 1997* and the *Commonwealth Authorities and Companies Act 1997* were replaced by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and supporting rules on 1 July 2014. The PGPA Act provides a common legislative framework for the governance, performance and accountability of all Commonwealth entities.

Substantially the content of this Guide, in particular the underlying concepts and principles of better practice, remain relevant. The ANAO will periodically review the currency of this Guide as part of the development of the Annual Work Program.

Further information on the PGPA Act is available at:

www.pmra.finance.gov.au

< BACK