Foreword

Establishing and monitoring internal controls over human resource (HR) information are important management functions. Internal control is fundamental to addressing risks to the completeness and accuracy of information and thus to providing assurance over the reliability of HR information, its compliance with applicable laws and regulations and the effectiveness and efficiency of operations.

Increasingly, entities are utilising Human Resource Management Information Systems (HRMIS) to assist in managing their workforce and in meeting their employer obligations. The effective discharge of these responsibilities is necessary to support the development and implementation of government programs and activities. However, the integration of technology to support managing a modern workforce can introduce a range of information management risks. With this in mind, the Guide emphasises the important role of both system and manual controls in maintaining the integrity and confidentiality of HR information.

The 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. The Guide identifies better practice system controls, and describes manual or process controls that are relevant to support or strengthen the implementation of system controls.

The Guide discusses risks and controls associated with the design, implementation and maintenance of the HRMIS and will be useful to assist HR system managers and practitioners to:

- implement better practices to improve the effectiveness and efficiency of HR and payroll processes;
- strengthen system controls and appropriately manage and segregate user access to key system functions; and
- increase awareness of system controls within the PeopleSoft and SAP HR systems that are used by a large number of Australian Government entities.

Implementation of controls should have due regard to the cost benefit involved. Equally, reducing controls for cost-saving reasons should be carefully managed as the operating risk profile may be increased.

The Guide is supported by a Supplement available from the ANAO website. The Supplement provides better practice examples for implementing controls for the SAP and PeopleSoft HRMIS applications as the key HR systems used within Australian Government entities.

Ian McPhee
Auditor-General

February 2011
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>i</td>
</tr>
<tr>
<td>Chapter 1. Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Purpose of this Guide</td>
<td>3</td>
</tr>
<tr>
<td>Structure of this Guide</td>
<td>4</td>
</tr>
<tr>
<td>Key Human Resource functions and risks</td>
<td>5</td>
</tr>
<tr>
<td>Central themes in this Guide</td>
<td>6</td>
</tr>
<tr>
<td>Identifying relevant controls</td>
<td>9</td>
</tr>
<tr>
<td>Chapter 2. HR and payroll data management</td>
<td>11</td>
</tr>
<tr>
<td>Key control objectives</td>
<td>14</td>
</tr>
<tr>
<td>Legislative and compliance considerations</td>
<td>14</td>
</tr>
<tr>
<td>Managing master data</td>
<td>15</td>
</tr>
<tr>
<td>Feature article: HR information and good privacy practice</td>
<td>17</td>
</tr>
<tr>
<td>Chapter 3. Workforce management</td>
<td>29</td>
</tr>
<tr>
<td>Key control objectives</td>
<td>31</td>
</tr>
<tr>
<td>Legislative and compliance considerations</td>
<td>31</td>
</tr>
<tr>
<td>Employee commencements</td>
<td>32</td>
</tr>
<tr>
<td>Employee exits and terminations</td>
<td>35</td>
</tr>
<tr>
<td>Chapter 4. Payroll processing and administration</td>
<td>39</td>
</tr>
<tr>
<td>Key control objectives</td>
<td>41</td>
</tr>
<tr>
<td>Legislative and compliance considerations</td>
<td>42</td>
</tr>
<tr>
<td>Time reporting</td>
<td>43</td>
</tr>
<tr>
<td>Payroll accounting</td>
<td>47</td>
</tr>
<tr>
<td>Feature article: Implementing self-service functionality</td>
<td>55</td>
</tr>
<tr>
<td>Chapter 5. System maintenance and integration</td>
<td>57</td>
</tr>
<tr>
<td>Key control objectives</td>
<td>59</td>
</tr>
<tr>
<td>Legislative and compliance considerations</td>
<td>60</td>
</tr>
<tr>
<td>Managing system interfaces</td>
<td>61</td>
</tr>
<tr>
<td>Managing system rules</td>
<td>64</td>
</tr>
<tr>
<td>Managing software updates</td>
<td>69</td>
</tr>
<tr>
<td>Feature article: Managing and maintaining the HRMIS</td>
<td>70</td>
</tr>
<tr>
<td>Appendices</td>
<td>73</td>
</tr>
<tr>
<td>Index</td>
<td>91</td>
</tr>
</tbody>
</table>
Chapter 1.
Introduction

Purpose of this Guide  3
Structure of this Guide  4
Key Human Resource functions and risks  5
Central themes in this Guide  6
Identifying relevant controls  9
Chapter 1. Introduction

Purpose of this Guide

The HRMIS is important to strategic decision-making as well as supporting day-to-day operational planning and administration. The Guide is intended for HR practitioners and system managers and discusses significant risks and controls relevant to the effective management of key HR functions.

HR and payroll functions are closely linked and changes in one process may create issues in another. As such, there is an emphasis in this Guide on implementing controls to safeguard the privacy and integrity of information.

“The technology infrastructure is now in place and the key role for 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

Government imperatives and stakeholder requirements carry implications for managing the workforce. The recent Blueprint for the Reform of Australian Government Administration recommended an agenda for nine key areas and established that responsibilities of executive managers should include a commitment to ensuring that Information Technology (IT) systems are appropriately implemented and maintained. Several recommendations were made for entities to implement more effective governance frameworks and improve the efficiency of corporate functions.

Further, the Gershon Review recommended cross-departmental initiatives for the sharing of IT infrastructure. These initiatives are designed to improve the efficiency of the delivery of government services, but may also increase both risk and the need for more sophisticated governance processes between entities.

4 The Online Supplement is available for download at the ANAO website, or an electronic version is available by contacting the ANAO on 02 6203 7300 or via email on: publications@anao.gov.au.
Structure of this Guide

The Human Resource Management Information Systems – Risks and Controls Better Practice Guide is divided into two parts, the Guide and an Online Supplement. Both parts are structured according to key HR functions and activities. The Guide discusses significant risks and controls relevant to key HR functions, and contains three feature articles that provide additional relevant discussion on aspects of managing HR information, implementing self-service functionality and managing the HRMIS.

The Online Supplement provides additional detail relevant to entities using either the Oracle PeopleSoft or the SAP ECC 6.0 installation of the relevant HRMIS. It provides additional detail concerning better practice and control guidelines when implementing and using these HRMIS installations.

Figure 1 depicts the above structure:

Figure 1: Better Practice Guide Structure
Key Human Resource functions and risks

The major chapters of the Guide provide an overview of significant risks and controls that are relevant to key HR functions. Establishing and monitoring the effectiveness of internal controls are important management functions and each chapter of the Guide provides details of better practice controls that are relevant to mitigating risks.

Chapter 2. HR and payroll data management

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

Chapter 3. Workforce management

Workforce management is a key strategic consideration within government entities. As with most other organisations, human capital is considered a significant asset, and the recruitment and maintenance of the right workforce is the key to success for operational and strategic objectives.

The chapter focuses on workforce management activities within a HRMIS to strengthen processes associated with the collection and maintenance of employee information, and in this context, the main activities that are discussed are:

- Employee commencements; and
- Employee exits and terminations.

Chapter 4. Payroll processing and administration

Payroll processing and administration is highly dependent on a number of inter-linking HR functions. The HRMIS provides a number of functions in performing payroll calculations that are crucial to ensuring that calculations are accurately performed. There are a number of supporting controls, particularly relevant to payroll disbursement and posting of payroll expenses to the General Ledger.

The chapter discusses risks and controls relevant to:

- Time reporting;
- Payroll accounting; and
- Processing of applicable deductions.

Chapter 5. System maintenance and integration

There are a number of functions and configuration options that can be used within an HRMIS to enhance the control environment or to increase efficiency within HR management processes. The chapter recognises that 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.

Topics covered include:

- Managing system interfaces;
- Managing system rules; and
- Managing software updates.
Central themes in this Guide

The HR function is the custodian of a variety of sensitive employment data and information. In this context, identifying significant risks and implementing effective system controls are essential to safeguard the integrity of this information. There are several key areas that should be considered:

- Managing HR and payroll data;
- Legislation and compliance; and
- Risks and controls.

The relevance of these areas to chapters of this Guide is discussed below.

Managing HR and payroll data

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

HR and payroll data are important to effective management of the human resource function, as they underlie every transaction conducted. Effective controls over employee information and master data is essential to maintain the integrity and confidentiality 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 requires Australian Government entities to protect information resources, including Information and Communication Technology (ICT) systems, from compromise and misuse. In addition, the Australian Government ICT Security Manual (ISM) outlines a combination of physical, personnel, information, IT and communications measures to assist entities to implement IT security controls that satisfy the minimum standards required to protect information stored or transmitted via electronic means.

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.

The Online Supplement to this Guide discusses security risks and recommendations for optimising security and access controls for the HR functionality supported by Oracle PeopleSoft and SAP applications. Security controls in both applications are inherently complex and require considerable knowledge and skill to implement.

Australian Government entities are required to comply with the Information Privacy Principles. 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 compliance

Given the current demand for both the disbursement of payroll and associated payments to be made electronically as well as for certain HR information to be exchanged electronically, effective controls over managing employee information and processing the payroll reduce the likelihood of errors or potential non-compliance with legislation.

Information maintained by government HR teams is a key input to internal management reports. In addition the Annual Report, incorporating the Financial Statements, includes a report of SES Remuneration and an overview of workforce composition. Further, entities are required to provide information for a range of Australian Government reports, such as the State of the Service Report.

Relevant legislation or compliance requirements for Australian Government entities are discussed with consideration to the purpose of the legislation and its usage in Government. Appendix 2 provides an overview of relevant legislation.

---


8 Further information is accessible at: http://www.privacy.gov.au
Risks and controls

The Guide provides an overview of the key HR functions being discussed and introduces relevant risks and 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 entities to mitigate such risks.

Risks relevant to the HR function are discussed and better practice controls recommended to mitigate these risks. Risks and controls are identified in this Guide using an ‘R’ for risk and each is given a unique number for easy identification. Each chapter 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, where relevant, often manual in nature, which are related to other HR processes are discussed under the section heading: Optimising the control environment.

There are significant HR risks surrounding segregation of duties. Segregation of duties is one of the key concepts of internal control as well as being a sound management practice. At its basic level, segregation implies that no individual is in a position to initiate, approve and review the same HR activity. In reality this requirement is often difficult to implement and sometimes costly to achieve.

Good segregation has as its primary objective the prevention of fraud and errors, and is a critical consideration when assigning system and user access. The objective is achieved by distributing key HR activities among multiple individuals and/or limiting the number of individuals with access to incompatible activities, e.g. managing HR master data and payroll processing. Often compensating controls will be required to manage or monitor the risks.

Control mechanisms available to assist with implementing effective segregation include:

- Audit trails;
- Reconciliations;
- Exception reports; and
- Supervisory review.

System and manual controls

Within this Guide, system controls are denoted by an ‘S’ preceding a reference number and are numbered within the range 1 to 39. Manual controls are denoted by an ‘M’ preceding a reference number and are numbered within the range 50 to 65.

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 Online Supplement provides detail on suggested better practice implementation of system controls for the ‘PeopleSoft’ and ‘SAP’ applications.
Managers controls

Manual controls (also called process controls) are a discretionary management or monitoring practice that may be performed by an entity. 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.

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.
- **Compliance and Reporting Risk**: a risk that the entity could be in breach of Australian legislative or regulatory requirements.
- **Fraud Risk**: a risk that an intentional deception could be made for personal gain, or to damage another individual or the entity.
- **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.

Appendix 3 provides a summary of the HR risks and controls discussed in this Guide.
Identifying relevant controls

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

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

Risks identified in this Guide that are related to the HR function are not all equal in likelihood, impact or in financial significance. The consideration to implement controls should have due regard to the cost benefit of mitigating identified risks.

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 the existence of 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 could create a single point of failure.
- Preventive 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.
- Automated controls are generally more reliable than manual or process controls and the reliability of automated controls is dependent upon an entity maintaining an effective control environment. For example, automated controls that force periodic changes to user passwords are more reliable than generic policies.

Customisation vs configuration

The Gershon Review of 2008 stated that “Many submissions indicated that there are no specific inhibitors to using commercial-off-the-shelf (COTS) solutions without customisation…there is often unnecessary excessive customisation by agencies. This erodes the inherent benefits offered by commercial off-the-shelf products, and increases costs.” The report noted that as a means to reduce expenditure, entities should reduce expenditure associated with customisation of software.

For the purposes of this Guide:

- **Customisation** is defined as programming changes made to the application that directly change the source code or the underlying table structures. Customisation may cause an increase in costs due to the difficulty of subsequent upgrades and could hinder future adoption of new features or functions that may be offered in later software releases.
- **Configuration** is defined as parameter changes that can be made without manipulating the source code or underlying table structures. Configuration is a non-invasive change to software settings or options that alters the business logic and configuration.

The system controls identified in the Online Supplement of this Guide as better practice considerations for implementation of effective system controls relate to available functionality, and do not require customisation.

---

9 Review of the Australian Government’s Use of Information and Communications Technology, August 2008, p.35.
Chapter 2.
HR and payroll data management

Key control objectives 14
Legislative and compliance considerations 14
Managing master data 15
*Feature article: HR information and good privacy practice* 17
Chapter 2. HR and payroll data management

This chapter focuses more broadly on general practices for appropriate maintenance of HR and payroll data. Other chapters of this Guide address risks and controls associated with management of transactions, or management of certain types of HR data. The importance of master data and its linkages to other HR processes discussed in this Guide is outlined in Figure 2 below. In addition, the feature article presents HR information and good privacy practice.

Input and maintenance of HR and payroll data is a significant area of risk. 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.

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 subject to regular change and update (e.g. performance management).

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

Master data is information that is critical to the operation of the HR function. Master data 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, banking details, 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 and update and is important for planning, decision-making or historical references. Typically, reference data includes information contained in audit logs.

Often the terms are used interchangeably. For example, taxation rates are a key table in an HRMIS and their function may be described as either reference data or master data. Generally, this Guide refers to master data, however the principles and risks apply to all data types that are entered, modified and stored in a HRMIS.

---

**Figure 2: Master data and linkages to HR processes**

---

[Diagram showing linkages between workforce management, HR and payroll data management, payroll processing and administration, employee commencements, exits and terminations, HRMIS master data, payroll processing, deductions, and employee benefits.]
Key control objectives

<table>
<thead>
<tr>
<th>Control objective</th>
<th>Risks mitigated</th>
</tr>
</thead>
<tbody>
<tr>
<td>HR and payroll data is appropriately maintained to provide accurate and complete employee information and payroll transactions.</td>
<td>R201: HR master data is inaccurate. R202: HR master data is not secure.</td>
</tr>
</tbody>
</table>

Legislative and compliance considerations

Safeguarding the privacy of employee information is an important consideration. Requirements of the Information Privacy Principles for the Australian Government are outlined in the feature article on *HR Information and good privacy practice*. 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 prospective, current and future employees. Additionally, there are obligations on entities to comply with the Australian Government Protective Security Framework and implement general practices generally to ensure that information is appropriately safeguarded.
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

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
<th>Better practice</th>
</tr>
</thead>
</table>
| R201: HR master data is inaccurate | Employee details may be incorrectly entered or maintained, which may result in duplicate payments, or errors with superannuation contributions or employee deductions, or unapproved changes to the allocation of roles or delegations. | System controls  
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 entry is entered.  
S02: Restricting user access to view, establish and amend 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). Implementing this control will prevent the data from being established.  
Manual controls  
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). |
R202: HR master data is not secure

<table>
<thead>
<tr>
<th>Risk type</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</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.</td>
</tr>
</tbody>
</table>

Implementing appropriate user access controls requires:

- Identification and implementation of segregation of duty requirements to validate update/modify/delete 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, vacation hours, and hire date) for their own records. With Web Client applications (self-service), 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 Employee Self Service 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.

Control S02. Restricting user access to view, establish and amend master data is also relevant.

Manual controls

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

<table>
<thead>
<tr>
<th>Control item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean desk policy and appropriate filing of hard copy employee records</td>
<td>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.</td>
</tr>
</tbody>
</table>
Feature article: 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 entities are required to comply with the eleven ‘Information Privacy Principles’ under section 14 of The Privacy Act 1988 (Cth). These Information Privacy Principles are reproduced at the end of this article.

A separate set of principles, the ‘National Privacy Principles’ apply to some private sector organisations. If agencies outsource their HR functions to a private sector organisation, the service 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: www.oaic.gov.au

Information Privacy Principles

A summary of the eleven 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 |

10 The ANAO acknowledges the input of the Office of the Australian Information Commissioner in reviewing this article.

11 This feature article refers to the term ‘agency’ rather than the term entity that is used throughout other sections of this Guide. This change in reference is deliberate in order to maintain consistency with references used in the legislation.
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:

“(a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of [the agency]; and

(b) the 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, entities 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 entities), 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);
- “the purpose for which each type of record is kept”;
- “the classes of individuals about whom records are kept”;
- “the period for which each type of record is kept”;
- “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
- “the 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

| Entities 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.

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:

(a) are accurate; and

(b) 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 a 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 etc 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 IPP 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

Information Privacy Principles 9 and 10 restrict the use that agencies can make 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 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**

**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:
(c) the purpose for which the information is being collected;
(d) 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
(e) 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 firstmentioned 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.
**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.
**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.
**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:
   (a) the 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) the individual concerned has consented to the disclosure;
   (c) the 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) the disclosure is required or authorised by or under law; or
   (e) 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.

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.
Chapter 3. Workforce management

Key control objectives 31
Legislative and compliance considerations 31
Employee commencements 32
Employee exits and terminations 35
Chapter 3. Workforce management

This chapter discusses activities relating to engagement of employees, managing promotions and transfers, and employee departures. Implementing effective controls in these areas are important to appropriately maintain employee information in the entity’s HRMIS and to ensure that payroll processing is accurate. Risks and controls for appropriately safeguarding employee related information is discussed under HR and payroll data management.

Workforce management is a key strategic consideration for government entities. Workforce management covers a range of activities and may include actions such as: recruitment of employees, learning and development, succession planning, and rewards and recognition.

Key control objectives

<table>
<thead>
<tr>
<th>Control objective</th>
<th>Risks mitigated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriate and accurate employee information is collected and maintained.</td>
<td>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.</td>
</tr>
</tbody>
</table>

Legislative and compliance considerations

Activities undertaken within the workforce management process are subject to various legislative and compliance requirements. The following table provides an overview of key legislation that is relevant to Workforce Management procedures. See the list of general legislation at Appendix 2.

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Service Act 1999</td>
<td>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.</td>
</tr>
<tr>
<td>Public Service Regulations 1999</td>
<td>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 SES and non-SES employee for a specified term (Part 3) and terms and conditions of employment of APS employees after machinery of government changes (Part 8).</td>
</tr>
<tr>
<td>Public Service Commissioner’s Directions 1999</td>
<td>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).</td>
</tr>
<tr>
<td>Public Service Classification Rules 2000</td>
<td>The Classification Rules detail the permitted classifications of APS employees and requirements around moving employees from training classifications to ordinary classifications.</td>
</tr>
</tbody>
</table>
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 new hire.

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 the new employee address to planned working time and salary and leave entitlements.

Given the sensitive content of employee conditions of employment it is important to consider the principles detailed in the Australian Government Information Privacy Principles. Principle 4 requires a record-keeper (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.

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 job within the same entity (or agency); or
- Inter-agency: An APS employee moving from one entity (or agency) 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.

A broader definition of intra-agency transfer refers to an employee permanently changing position or working in a different position on a temporary basis (for example, covering another employee’s extended absence or working in a higher duty capacity than their stipulated role). Ensuring master data and time accurately reflects the position in which all employees are working is referred to as Position Management.

Position management

Employees are allocated to a particular role or position in the HRMIS. 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 System maintenance and integration.
### Risks and controls

| R301: Non-existent or duplicate employee is added to the payroll |
|---|---|
| **Risk type** | ![lock](image) ![location](image) ![currency](image) |
| **Impact** | ‘Ghost’ or duplicate employees on the payroll lead to overpayment or processing of fraudulent payments. |
| **Better practice** | **System Controls**

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.

**Manual Controls**

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 hire, employee information including bank account) to validate the set-up was authorised and has been completed accurately.

Risks and controls associated with inter-agency transfers are similar to risks associated with the employee commencement and exit process that is discussed in [Employee exits and terminations](#). 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. The effect of transfers on the organisational chart is addressed in [System maintenance and integration](#).
## 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 the discussion on System maintenance and integration.

The following items should be considered to enhance the maintenance of the employee commencement process:

<table>
<thead>
<tr>
<th>Control item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development of standardised reference and background check procedures</td>
<td>A security clearance and reference checking policy should be developed and documented. 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.</td>
</tr>
<tr>
<td>Information collected during the application process is handled in accordance with Privacy legislation</td>
<td>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.</td>
</tr>
<tr>
<td>Managing transfer requirements</td>
<td>Part 11 of the Financial Management and Accountability Regulations 1997 stipulates arrangements for transfer of employee leave entitlements when employees move between agencies.</td>
</tr>
<tr>
<td>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.</td>
<td>A new hire 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.</td>
</tr>
</tbody>
</table>
Employee exits and terminations

The employee exit process is initiated when either the employer or employee provides notice of termination. During an employee’s notice period, key tasks undertaken are completion of operational responsibilities, knowledge transfer and an exit interview between employer and employee.

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

<table>
<thead>
<tr>
<th>R302: Termination payments and balances are inaccurately calculated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk type</td>
</tr>
<tr>
<td>Impact</td>
</tr>
<tr>
<td>Better practice</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### R303: Employee is not inactivated when employment is terminated

| Risk type | Impact | Better practice |
|-----------|--------|-----------------
|           | Employee record is not flagged as terminated which may result in subsequent payment to the employee. For entities 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. | **System Controls**

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.

**Manual Controls**

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:

<table>
<thead>
<tr>
<th>Control item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘Employee Exit’ checklist</td>
<td>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.</td>
</tr>
<tr>
<td>Reconciliation of terminations</td>
<td>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.</td>
</tr>
</tbody>
</table>
Chapter 4. Payroll processing and administration

Key control objectives 41
Legislative and compliance considerations 42
Time reporting 43
Payroll accounting 47
Feature article: Implementing self-service functionality 55
Chapter 4. Payroll processing and administration

This chapter discusses risks and controls relative to the accuracy and completeness of payroll processing and includes HR activities related to time recording and payroll accounting. Extensive reference is made to legislation related to payroll deductions and superannuation. The feature article discusses implementing self-service functionality.

The payroll processing and administration is highly dependent on a number of inter-linking 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.

### Key control objectives

<table>
<thead>
<tr>
<th>Control objective</th>
<th>Risks mitigated</th>
</tr>
</thead>
</table>
| 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 work rosters within the HR system are updated inaccurately.  
R404: Time recorded in prior periods is amended inaccurately or without appropriate authority. |
| Accurately 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 bonus payments or other rewards are accurately, calculated and appropriately approved prior to disbursement. | R409: Methodology for bonus rewards is not established.  
R410: Employee benefits are not managed or administered in accordance with Workplace Agreements/employee contracts. |
## Legislative and compliance considerations

Activities undertaken by the payroll processing and administration process are subject to various legislative and compliance requirements. The following table provides an overview of key legislation that is relevant to payroll processing and administration procedures. See also the list of general legislation at Appendix 2.

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long Service Leave (Commonwealth Employees) Act 1976</td>
<td>Sets out the conditions of eligibility, accrual and payment of long service leave for Commonwealth employees.</td>
</tr>
<tr>
<td>Maternity Leave (Commonwealth Employees) Act 1973</td>
<td>Sets out the paid and unpaid maternity leave arrangements for Commonwealth employees. Employers often provide supplementary maternity leave benefits in collective/enterprise agreements.</td>
</tr>
<tr>
<td>Safety Rehabilitation and Compensation Act 1988</td>
<td>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.</td>
</tr>
<tr>
<td>Superannuation (Productivity Benefit) Act 1988</td>
<td>Provides for Productivity Benefit contributions and payments in relation to certain employees of the Commonwealth who were employed before 1 July 2006.</td>
</tr>
<tr>
<td>Superannuation Act 1976</td>
<td>Sets out the superannuation arrangements that are applicable to members of the Commonwealth Superannuation Scheme (a defined benefits superannuation scheme) including in relation to the contributions employers are required to make.</td>
</tr>
<tr>
<td>Superannuation Act 1990</td>
<td>Sets out the superannuation arrangements that are applicable to members of the Public Sector Superannuation Scheme (a defined benefits superannuation scheme). This Act should be read in conjunction with the “Deed to Establish an Occupational Superannuation Scheme for Commonwealth Employees and Certain Other Persons (the Public Sector Superannuation Scheme)” which contains Rules setting out matters including the amount of contributions required to be made and how members’ benefits are calculated.</td>
</tr>
<tr>
<td>Superannuation Act 2005</td>
<td>Sets out the superannuation arrangements that are applicable to members of the Public Sector Superannuation (Accumulation Plan) Scheme (an accumulation plan scheme). This Act should be read in conjunction with the “Superannuation (PSSAP) Trust Deed” which contains Rules setting out matters including the amount of contributions required to be made and how members’ benefits are calculated.</td>
</tr>
<tr>
<td>Superannuation Guarantee (Administration) Act 1992</td>
<td>Provides for the establishment and administration of the Superannuation Guarantee Scheme which provides incentives for employers to make certain minimum superannuation contributions in respect of their employees.</td>
</tr>
<tr>
<td>Taxation Administration Act 1953</td>
<td>Schedule 1 to the Act details the withholding obligations on employers in relation to payments made to employees. These obligations are required to be met in order to comply with the PAYG withholding regime. The rates of withholding are calculated in accordance with the provisions of the Part 5 of the Regulations.</td>
</tr>
</tbody>
</table>
**Time reporting**

The capture of employee time allocations and leave is essential to the accurate processing of payroll and related financial reporting.

Time reporting captures the duration of employees’ working hours for a defined time period—weekly, fortnightly, monthly. 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.

**Risks and controls**

<table>
<thead>
<tr>
<th>R401: Inaccurate or incomplete entry of employee time data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk type</strong></td>
</tr>
<tr>
<td>Time data entered does not accurately reflect time worked or does not include leave taken.</td>
</tr>
<tr>
<td>Employee receives payment for hours or leave to which they are not entitled.</td>
</tr>
<tr>
<td><strong>Impact</strong></td>
</tr>
<tr>
<td>System controls</td>
</tr>
<tr>
<td><strong>Better practice</strong></td>
</tr>
<tr>
<td>S12: Workflow approval of employee time.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>S13: System validation of data entered.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>S14: Timesheets are locked for editing after submission.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>S15: Automated notifications.</td>
</tr>
<tr>
<td>Automated notifications remind users to enter their time report, and continue to alert users when the time reporting deadline is reached and passed.</td>
</tr>
<tr>
<td>Manual controls</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
### R402: Unapproved leave or leave is taken outside of entitlements

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
<th>Better practice</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Employee takes leave which is either not recorded on timesheets, or when recorded results in the employee having a negative leave balance.</td>
<td><strong>System controls</strong>&lt;br&gt;S16: <em>Automated checks on leave applications to confirm sufficient entitlement.</em>&lt;br&gt;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.&lt;br&gt;S17: <em>Workflow approval of leave requests.</em>&lt;br&gt;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.&lt;br&gt;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.&lt;br&gt;Also refer to S37: <em>Organisational chart designed to reflect the hierarchy</em> on page 67. <strong>Manual controls</strong>&lt;br&gt;M56: <em>Periodic review over recording of leave.</em>&lt;br&gt;A two-way check should be performed by the payroll team on a monthly basis to confirm that:&lt;br&gt;• Leave taken by employees is reflected in timesheets; and&lt;br&gt;• Leave recorded was appropriately approved.&lt;br&gt;Any discrepancies should be followed up with the employee and the employee’s immediate supervisor.</td>
</tr>
</tbody>
</table>

### R403: Established work rosters within the HR system are updated inaccurately

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
<th>Better practice</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inaccurate employee rosters lead to inaccurate payroll processing and may impact leave accrual calculations.</td>
<td><strong>System controls</strong>&lt;br&gt;S18: <em>Restrict user access to amend work rosters.</em>&lt;br&gt;Access to update work rosters should be restricted to appropriate personnel and employees should not have access to update their own work roster. <strong>Manual controls</strong>&lt;br&gt;M57: <em>Approval of updates to work rosters.</em>&lt;br&gt;Work rosters should only be updated in the system following approval by an appropriate authority.</td>
</tr>
<tr>
<td>Risk type</td>
<td>Impact</td>
<td>Better practice</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
|           | Inaccurate or unauthorised adjustments lead to inaccurate leave balances or time reporting. | **System controls**<br><br>S19: *Restrict user access to process prior period adjustment.*<br>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.<br><br>S20: *Workflow approval of prior period adjustments.*<br>Amendments to time recorded in prior periods should be processed through the workflow approval hierarchy.<br><br>S21: *Limit prior period adjustments.*<br>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).  
**Manual controls**<br><br>M58: *Approval of prior period adjustments prior to processing.*<br>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.<br><br>M59: *Review prior period adjustments.*<br>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:

<table>
<thead>
<tr>
<th>Control item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use standard leave forms</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Authorisation of amended timesheets</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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 3: 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.
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, provision of car parking, or paying an employee’s private health insurance costs. 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.\(^\text{12}\)

**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).\(^\text{13}\)

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.

---

\(^{12}\) See list of relevant superannuation legislation discussed earlier in the Legislative and compliance considerations section.

**Defined benefit schemes**

Australian Government employees who commenced employment prior to 1 July 1990 or 1 July 2005 may be members of the Commonwealth Superannuation Scheme (CSS) or Public Sector Superannuation (PSS) scheme respectively. The CSS and PSS are defined benefit superannuation schemes. Administration of defined benefit schemes 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 entities 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.

**Bonus payments**

Bonus payments are cash payments typically made on an annual basis and disbursed in conjunction with the standard payroll processing discussed earlier.

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 bonus 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 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 for accrual and calculation purposes.

**Other benefits**

Other benefits may be available to employees in addition to their salary or wage. 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 contract or Workplace Agreement. Common additional benefits offered include access to lower premiums for private health insurance, corporate mobile phone plans and health club memberships.

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.
## Risks and controls

### R405: Payroll calculation is inaccurate or incomplete

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft payroll proposals are not reviewed for reasonableness prior to finalisation of the payroll, resulting in failure to detect significant anomalies or errors.</td>
<td></td>
</tr>
</tbody>
</table>

**Better practice**

**System controls**

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.

**Manual controls**

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

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

**Better practice**

**System controls**

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.

**Manual controls**

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

<table>
<thead>
<tr>
<th>Risk type</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</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>System controls</td>
</tr>
<tr>
<td></td>
<td>S24: Configure automated calculation of superannuation payable.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

### R408: Salary sacrifice arrangements are not appropriately managed

<table>
<thead>
<tr>
<th>Risk type</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>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.</td>
</tr>
<tr>
<td>Better practice</td>
<td>System controls</td>
</tr>
<tr>
<td></td>
<td>S25: Salary sacrifice details are appropriately established in the HRMIS.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Manual controls</td>
</tr>
<tr>
<td></td>
<td>M62: Review and monitor changes to key salary sacrifice information.</td>
</tr>
<tr>
<td></td>
<td>Set-up of the salary package elements and rules should be independently reviewed to ensure the following:</td>
</tr>
<tr>
<td></td>
<td>• Configuration accurately reflects the documented salary sacrifice agreement;</td>
</tr>
<tr>
<td></td>
<td>• The salary/wage component has been accurately captured to enable accurate PAYG withholding;</td>
</tr>
<tr>
<td></td>
<td>• Sacrifices which constitute fringe benefits have been accurately classified and captured to enable accurate Fringe Benefits Tax self-assessment;</td>
</tr>
<tr>
<td></td>
<td>• 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</td>
</tr>
<tr>
<td></td>
<td>• Salary package elements outside the policy framework are not included as part of the arrangement.</td>
</tr>
</tbody>
</table>
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\textsuperscript{14}. Automated updates should be configured to assist in ensuring tax information remains current (see \textit{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\textsuperscript{15}. Employees who are members of accumulated contribution schemes will be flagged as such, and the defined percentage\textsuperscript{16} 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.

\begin{center}
\begin{tabular}{|l|p{0.8\textwidth}|}
\hline
\textbf{R409: Methodology for bonus rewards is not established} & \\
\hline
\textbf{Risk type} & \includegraphics[width=0.05\textwidth]{blue-dollar}\includegraphics[width=0.05\textwidth]{cloud} & \\
\hline
\textbf{Impact} & Unauthorised or inaccurate bonus payments may be disbursed to employees. \\
 & Bonuses may not be adequately accounted for throughout the period. & \\
\hline
\textbf{Better practice} & \textbf{System controls} & \\
S26: \textit{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. & \\
\hline
\end{tabular}
\end{center}

\textsuperscript{14} Refer to www.ato.gov.au for tax withholding tables.
\textsuperscript{15} The amount to be contributed for each employee is set out in an annual letter from the Department of Finance and Deregulation.
\textsuperscript{16} The percentage payable at the time of publishing is 15.4\%, as governed by the Australian Government Department of Finance and Deregulation, under the legal authority of the Superannuation Act 2005.
<table>
<thead>
<tr>
<th>Risk type</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
| Better practice | System controls  
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. |
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:

<table>
<thead>
<tr>
<th>Control item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop policy around information retention</td>
<td>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.</td>
</tr>
<tr>
<td>Salary sacrifice policy</td>
<td>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.</td>
</tr>
<tr>
<td>Dual authorisation to disburse payments</td>
<td>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.</td>
</tr>
<tr>
<td>Automated interface of EFT file to banking application</td>
<td>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.</td>
</tr>
<tr>
<td>Reconciliation of disbursement amount to approved ledger</td>
<td>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).</td>
</tr>
<tr>
<td>Record, authorise and review benefit plans</td>
<td>Changes to employee benefits should be recorded and approved appropriately prior to the changes being implemented in the HRMIS.</td>
</tr>
</tbody>
</table>
Feature article: 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.

Determine 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.

Provide 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.

**Educate 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.

**Establish 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.

**Implement 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.

**Develop 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.
Chapter 5.
System maintenance and integration

Key control objectives  59
Legislative and compliance considerations  60
Managing system interfaces  61
Managing system rules  64
Managing software updates  69
Feature article: Managing and maintaining the HRMIS  70
# Chapter 5. System maintenance and integration

This chapter outlines additional configuration aspects of the HRMIS to improve management of system interfaces, business rules and software updates. The feature article at the end of the chapter discusses better practice considerations for maintaining an effective control environment for the HRMIS.

## Key control objectives

<table>
<thead>
<tr>
<th>Control objective</th>
<th>Risks mitigated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll information is completely and accurately posted to the General Ledger via the payroll journal.</td>
<td>R501: Payroll system does not reconcile to the General Ledger.</td>
</tr>
<tr>
<td>Information regarding superannuation contributions is submitted to superannuation funds (such as ComSuper) via an automated interface, ensuring complete and accurate transfer of data.</td>
<td>R502: Incomplete or inaccurate submission of superannuation data.</td>
</tr>
<tr>
<td>The rate at which leave accrues and leave types to which employees are entitled is accurately established.</td>
<td>R503: Leave accrual rates are established inaccurately.</td>
</tr>
<tr>
<td>Fields requiring translation into a foreign currency correctly reference accurate foreign exchange rates within the HRMIS to enable accurate calculations.</td>
<td>R504: Employee wages paid in foreign currency are calculated incorrectly.</td>
</tr>
<tr>
<td>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.</td>
<td>R505: The HR system organisational chart does not accurately reflect current employees and their positions.</td>
</tr>
<tr>
<td>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.</td>
<td>R506: Payroll schemas established or modified inaccurately or without authorisation.</td>
</tr>
<tr>
<td>Risks to business systems are generally reduced when available patches are installed in a timely manner after being tested for reliability and usability.</td>
<td>R507: Application is vulnerable to security or availability threats.</td>
</tr>
</tbody>
</table>
### Legislative and compliance considerations

The following table provides an overview of key legislation and guidelines/policy relevant to implementation of appropriate system and business rules. See also the list of general legislation at Appendix 2 and the superannuation and tax withholding legislation referred to in the previous chapter, *Payroll processing and administration.*

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commonwealth Procurement Guidelines (CPGs)</td>
<td>These guidelines impose obligations on Commonwealth Government entities when procuring goods and services. They are intended to ensure that the Commonwealth achieves value for money in its procurements and obtains goods and services from appropriate organisations. The CPGs apply to all agencies that are subject to the Financial Management and Accountability Act 1997 and some bodies that are subject to the Commonwealth Authorities and Companies Act 1997. The CPGs are particularly relevant where any services (such as IT, HR or salary sacrifice) are being outsourced.</td>
</tr>
<tr>
<td>Financial Management and Accountability Act 1997</td>
<td>Addresses requirements in relation to the handling of public money (Part 3) and accounting and auditing requirements more generally (Parts 4, 7 and 8).</td>
</tr>
<tr>
<td>Financial Management and Accountability Regulations 1997</td>
<td>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. The Regulations cover a variety of auditing requirements.</td>
</tr>
<tr>
<td>Finance Minister’s Orders for Financial Reporting</td>
<td>Set out accounting policy and financial reporting requirements for Commonwealth Government entities.</td>
</tr>
</tbody>
</table>
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 impacted 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 and are discussed in the Optimising the control framework section.

There are several ways in which information is exchanged between information systems. Entities 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, entities use a HRMIS that is a separate product to other business and financial systems and this will mean that information is shared between systems via an interface. In some cases, entities 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 entities. Financial reporting is required to be prepared to comply with the Australian Accounting Standards, and the Finance Minister’s Orders.¹⁷ Payroll is a significant expense for most entities. 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.¹⁸ 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.¹⁹ 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.

---

¹⁷ For further information on the preparation of financial statements for the Australian public sector, refer to the Australian National Audit Office Better Practice Guide Preparation of Financial Statements by Public Sector Agencies June 2009.

¹⁸ 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 (MilitarySuper) scheme and the Defence Force Retirement and Death Benefits (DFRDB) scheme.

## Risks and controls

### R501: Payroll system does not reconcile to the General Ledger

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

### Better practice

**System controls**

- **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.

**Manual controls**

- **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

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Information submitted to the superannuation fund is incomplete or inaccurate, potentially leading to penalty payments or incorrect reporting of superannuation payments.</td>
</tr>
</tbody>
</table>

### Better practice

**System controls**

- **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:

<table>
<thead>
<tr>
<th>Control item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual payroll to General Ledger reconciliation</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 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 below:

<table>
<thead>
<tr>
<th>HRMIS Database Schema/Structure</th>
<th>HRMIS Master Data e.g. employee data</th>
<th>Rules e.g. taxation rules, superannuation rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>HRMIS Functions and Operations e.g. payroll processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payroll Results</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Overview of SAP and PeopleSoft HRMIS payroll configuration

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).

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.

The Online Supplement provides further detail on the particular schemas and rules relevant to the SAP and PeopleSoft payroll configuration.

---

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.
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 sick 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.

While the organisational chart is commonly available on an entity’s intranet, it should also be maintained in the HRMIS to facilitate HR activity.
### Risks and controls

#### R503: Leave accrual rates are established inaccurately

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
<th>Better practice</th>
</tr>
</thead>
</table>
|           | Inaccuracies in leave accruals reduce the accuracy and reliability of the payroll calculation and associated financial reports. | **System controls**  
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 Awards) 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.  
**Manual controls**  
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

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
<th>Better practice</th>
</tr>
</thead>
</table>
|           | Use of inaccurate foreign exchange rates for currency translation purposes will result in inaccurate calculation of payroll. | **System controls**  
S34: Establish automated updates for foreign exchange rates.  
An automated update of foreign exchange rates should be established between a reputable website and the entity application to ensure rates applied are up to date and accurate. |
### R505: The HR system organisational chart does not accurately reflect current employees and their positions

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
<th>Better practice</th>
</tr>
</thead>
</table>
|           | 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. | **System controls**  
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

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Impact</th>
<th>Better practice</th>
</tr>
</thead>
</table>
|           | 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. | **System controls**  
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. |
## Optimising the control environment

Better practice considerations for managing system rules are highlighted below:

<table>
<thead>
<tr>
<th>Control Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change management controls over payroll configuration</td>
<td>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.</td>
</tr>
<tr>
<td>Manage changes to system rules</td>
<td>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.</td>
</tr>
<tr>
<td>Independent verification of manually keyed foreign exchange rates</td>
<td>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.</td>
</tr>
<tr>
<td>Periodic review of salary/wage payments made in foreign currency</td>
<td>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.</td>
</tr>
<tr>
<td>Periodic review of HRMIS organisational chart</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>R507: Application is vulnerable to security and availability threats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk type</strong></td>
</tr>
<tr>
<td><strong>Impact</strong></td>
</tr>
</tbody>
</table>
| **Better practice** | **System controls**  
S39: *Automatic notification of available software updates.*  
Automatic notification should be configured to alert the system administrator whenever a software update is available.  
**Manual controls**  
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

Better practice guidance to assist in determining the effectiveness of important controls in the IT environment is provided in the following feature article.
Feature article: Managing and maintaining the HRMIS

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 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.

Further detail on system and configuration practices to consider in managing the HRMIS is discussed in **System maintenance and integration**. 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 the section titled ‘Managing system interfaces’ in **System maintenance and integration**.

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, entities must be confident that they have procedures in place to recover from such interruption, such that:

- entities 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.
Appendices

Appendix 1: Glossary 75
Appendix 2: Relevant Australian Government Legislation and external references 79
Appendix 3: Summary of HR functions with related risks and controls 83
Appendix 4: PeopleSoft and SAP HRMIS functionality 87
## Appendix 1: Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>The process of restricting access to particular HR Management Information System areas, transactions or functions to authorised users.</td>
</tr>
<tr>
<td>Audit report</td>
<td>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.</td>
</tr>
<tr>
<td>Automated control</td>
<td>Refer to System control.</td>
</tr>
<tr>
<td>Change management process</td>
<td>A model which outlines how changes to a system or organisation should be implemented in a controlled manner.</td>
</tr>
<tr>
<td>Configuration</td>
<td>The act of setting parameters in the system to control the business processes performed. The system must be configured to meet the needs of the entity before it can be used.</td>
</tr>
<tr>
<td>Configuration control</td>
<td>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.</td>
</tr>
<tr>
<td>Control objectives</td>
<td>Control objectives are high-level statements by management that provide a link between organisational risks and the internal controls and activities implemented by entities to mitigate such risks.</td>
</tr>
<tr>
<td>Controls</td>
<td>Policies, procedures and practices designed to mitigate and reduce the chance of risks being realised.</td>
</tr>
<tr>
<td>Cost centre</td>
<td>Organisational unit within a controlling area that represents a defined location of cost incurrence. The definition can be based on: Functional requirements, Allocation criteria, Physical location and Responsibility for costs.</td>
</tr>
<tr>
<td>Customisation</td>
<td>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.</td>
</tr>
<tr>
<td>Data</td>
<td>Representation of facts, concepts or instructions in a formalised manner suitable for communication, interpreting or processing by users or by automatic means.</td>
</tr>
<tr>
<td>Database</td>
<td>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.</td>
</tr>
<tr>
<td>Default</td>
<td>The configuration settings that are in place upon installation of the HRMIS.</td>
</tr>
<tr>
<td>Duplicate employees</td>
<td>An employee who is listed two or more times on the payroll.</td>
</tr>
<tr>
<td>Edit access</td>
<td>Access within an HR Management Information System to input, amend or delete data.</td>
</tr>
<tr>
<td>Employee contribution</td>
<td>Amounts contributed to superannuation funds in excess of the statutory employer contribution.</td>
</tr>
<tr>
<td>Employee Self Service (ESS)</td>
<td>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.</td>
</tr>
<tr>
<td>ESS</td>
<td>Refer Employee Self Service.</td>
</tr>
<tr>
<td>Field</td>
<td>A particular characteristic of a particular item that can be input/modified by a user.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Function</strong></td>
<td>A task that an employee performs to accomplish a specific portion of his/her job responsibilities. A function is a grouping of one or more 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.</td>
</tr>
<tr>
<td><strong>HRMIS</strong></td>
<td>Human Resource Management Information System.</td>
</tr>
<tr>
<td><strong>Human Resource Management Information System</strong></td>
<td>The information system that supports an entity's HR function, allowing the entity to automate tasks such as processing employee payments.</td>
</tr>
<tr>
<td><strong>ICT</strong></td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Within this Guide, used in the context of data, that is, data that is complete and accurate.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Logical access</strong></td>
<td>Refers to user or system access to data files or computer programs.</td>
</tr>
<tr>
<td><strong>Manager Self Service</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Master data</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Module</strong></td>
<td>Part of a program that performs a distinct function.</td>
</tr>
<tr>
<td><strong>MSS</strong></td>
<td>Manager Self Service.</td>
</tr>
<tr>
<td><strong>Oracle PeopleSoft</strong></td>
<td>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’.</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>Parameters define the way the HR Management Information System operates, particularly system logon and password maintenance functions.</td>
</tr>
<tr>
<td><strong>Software update</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Payroll calculation</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Payroll exception reporting</strong></td>
<td>Reporting which shows the difference between what was paid in the prior payroll period and what was paid in the current payroll period.</td>
</tr>
<tr>
<td><strong>Physical access</strong></td>
<td>Access to areas rather than to an IT system, for example, access to a building, room, filing cabinet, safe.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Position based security</td>
<td>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.</td>
</tr>
<tr>
<td>Prior period adjustment</td>
<td>An adjustment processed to a period which has been closed or finalised for timekeeping or accounting purposes.</td>
</tr>
<tr>
<td>Profile</td>
<td>A collection of authorisations which have been grouped together to be allocated to a user (to assign access capabilities).</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>Item by item examination of two related sets of figures obtained from different sources.</td>
</tr>
<tr>
<td>Risk</td>
<td>A combination of the likelihood of an adverse even occurring and the consequence that such an event may have on the entity.</td>
</tr>
<tr>
<td>Role</td>
<td>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.</td>
</tr>
<tr>
<td>SAP</td>
<td>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.</td>
</tr>
<tr>
<td>Segregation of duties</td>
<td>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.</td>
</tr>
<tr>
<td>Two functional duties conflict</td>
<td>Two functional duties that, if performed by the same user, increase the chances of fraud and/or error occurring.</td>
</tr>
<tr>
<td>Service Level Agreement</td>
<td>Contract between a service provider and a customer detailing the nature, quality, and scope of the service to be provided.</td>
</tr>
<tr>
<td>Single sign-on</td>
<td>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.</td>
</tr>
<tr>
<td>SLA</td>
<td>Refer to Service Level Agreement</td>
</tr>
<tr>
<td>SOD</td>
<td>Refer to Segregation of duties</td>
</tr>
<tr>
<td>SSO</td>
<td>Refer to Single sign-on</td>
</tr>
<tr>
<td>System control</td>
<td>A control performed automatically by an IT system. In order for this control to operate, it may need to be configured within the system.</td>
</tr>
<tr>
<td>Table</td>
<td>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.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Test environment</td>
<td>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.</td>
</tr>
<tr>
<td>Transaction codes</td>
<td>Various functions within the HR Management Information System are referred to as transactions. Most functions can be invoked by a transaction code.</td>
</tr>
<tr>
<td>Validation check</td>
<td>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.</td>
</tr>
<tr>
<td>View access</td>
<td>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.</td>
</tr>
<tr>
<td>Workflow</td>
<td>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.</td>
</tr>
</tbody>
</table>
# Appendix 2: Relevant Australian Government legislation and external references

The following table provides an overview of key legislation that is relevant to the human resource and payroll functions. Additional legislation is included where it is relevant to the Australian Government.

## Table 1: Legislation of general relevance

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commonwealth Fraud Control Guidelines 2002</strong></td>
<td>The Commonwealth Fraud Control Guidelines outline the principles of fraud control within the Commonwealth and set national minimum standards to assist Commonwealth entities to carry out their responsibilities to combat fraud in relation to their programs. The Guidelines outline the responsibilities of entities for fraud prevention, reporting of fraud information, fraud investigation case handling and training of entity fraud investigators and fraud prevention officers.</td>
</tr>
<tr>
<td><strong>Fair Work Act 2009</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Privacy Act 1988</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
The following is a list of all legislation that is referred to in this Guide. The list is not exhaustive and is intended as a reference for HR practitioners.

### Table 2: Legislation referred to in this Guide

<table>
<thead>
<tr>
<th>Legislation</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public Service Act 1999</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Public Service Regulations 1999</strong></td>
<td>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 SES and non-SES employee for a specified term (Part 3) and terms and conditions of employment of APS employees after machinery of government changes (Part 8).</td>
</tr>
<tr>
<td><strong>Public Service Commissioner’s Directions 1999</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Public Service Classification Rules 2000</strong></td>
<td>The Classification Rules detail the permitted classifications of APS employees and requirements around moving employees from training classifications to ordinary classifications.</td>
</tr>
<tr>
<td><strong>Long Service Leave (Commonwealth Employees) Act 1976</strong></td>
<td>Sets out the conditions of eligibility, accrual and payment of long service leave for Commonwealth employees.</td>
</tr>
<tr>
<td><strong>Maternity Leave (Commonwealth Employees) Act 1973</strong></td>
<td>Sets out the paid and unpaid maternity leave arrangements for Commonwealth employees. Employers often provide supplementary maternity leave benefits in collective/enterprise agreements.</td>
</tr>
<tr>
<td><strong>Safety Rehabilitation and Compensation Act 1988</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Superannuation (Productivity Benefit) Act 1988</strong></td>
<td>Provides for Productivity Benefit contributions and payments in relation to certain employees of the Commonwealth who were employed before 1 July 2006.</td>
</tr>
<tr>
<td><strong>Superannuation Act 1976</strong></td>
<td>Sets out the superannuation arrangements that are applicable to members of the Commonwealth Superannuation Scheme (a defined benefits superannuation scheme) including in relation to the contributions employers are required to make.</td>
</tr>
<tr>
<td><strong>Superannuation Act 1990</strong></td>
<td>Sets out the superannuation arrangements that are applicable to members of the Public Sector Superannuation Scheme (a defined benefits superannuation scheme). This Act should be read in conjunction with the “Deed to Establish an Occupational Superannuation Scheme for Commonwealth Employees and Certain Other Persons (the Public Sector Superannuation Scheme)” which contains Rules setting out matters including the amount of contributions required to be made and how members’ benefits are calculated.</td>
</tr>
<tr>
<td>Legislation</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>Superannuation Act 2005</td>
<td>Sets out the superannuation arrangements that are applicable to members of the Public Sector Superannuation (Accumulation Plan) Scheme (an accumulation plan scheme). This Act should be read in conjunction with the “Superannuation (PSSAP) Trust Deed” which contains Rules setting out matters including the amount of contributions required to be made and how members’ benefits are calculated.</td>
</tr>
<tr>
<td>Superannuation Guarantee (Administration) Act 1992</td>
<td>Provides for the establishment and administration of the Superannuation Guarantee Scheme which provides incentives for employers to make certain minimum superannuation contributions in respect of their employees.</td>
</tr>
<tr>
<td>Taxation Administration Act 1953</td>
<td>Schedule 1 to the Act details the withholding obligations on employers in relation to payments made to employees. These obligations are required to be met in order to comply with the PAYG withholding regime. The rates of withholding are calculated in accordance with the provisions of the Part 5 of the Regulations.</td>
</tr>
<tr>
<td>Tax Administration Regulations 1976</td>
<td></td>
</tr>
<tr>
<td>Commonwealth Procurement Guidelines (CPGs)</td>
<td>These guidelines impose obligations on Commonwealth Government entities when procuring goods and services. They are intended to ensure that the Commonwealth achieves value for money in its procurements and obtains goods and services from appropriate organisations. The CPGs apply to all agencies that are subject to the Financial Management and Accountability Act 1997 and some bodies that are subject to the Commonwealth Authorities and Companies Act 1997. The CPGs are particularly relevant where any services (such as IT, HR or salary sacrifice) are being outsourced.</td>
</tr>
<tr>
<td>Financial Management and Accountability Act 1997</td>
<td>Addresses requirements in relation to the handling of public money (Part 3) and accounting and auditing requirements more generally (Parts 4, 7 and 8).</td>
</tr>
<tr>
<td>Financial Management and Accountability Regulations 1997</td>
<td>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. The Regulations cover a variety of auditing requirements.</td>
</tr>
<tr>
<td>Finance Minister’s Orders for Financial Reporting</td>
<td>Set out accounting policy and financial reporting requirements for Commonwealth Government entities.</td>
</tr>
</tbody>
</table>
The following table lists key websites that provide additional background or reference information relevant to areas covered by this Guide.

### Table 3: External references

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>ComSuper</td>
<td><a href="http://employer.pss-css.gov.au/">http://employer.pss-css.gov.au/</a></td>
<td>This site provides information and tools to assist employers administer super for members of the Australian Government Superannuation Scheme.</td>
</tr>
<tr>
<td>Office of the Australian Information Commissioner</td>
<td><a href="http://www.oaic.gov.au">http://www.oaic.gov.au</a></td>
<td>This site provides information on the functions of the Privacy Commission.</td>
</tr>
<tr>
<td>Australian Taxation Office</td>
<td><a href="http://www.ato.gov.au/">http://www.ato.gov.au/</a></td>
<td>This site provides information on the Taxation Office’s functions and compliance requirements for tax.</td>
</tr>
<tr>
<td>Department of Finance and Deregulation</td>
<td><a href="http://www.finance.gov.au/index.html">http://www.finance.gov.au/index.html</a></td>
<td>This site provides information on the financial model for Australian Government entities.</td>
</tr>
<tr>
<td>Department of Education, Employment and Workplace Relations</td>
<td><a href="http://www.deewr.gov.au/WorkplaceRelations/Pages/default.aspx">http://www.deewr.gov.au/WorkplaceRelations/Pages/default.aspx</a></td>
<td>This site provides information on Australia’s Fair Work System.</td>
</tr>
</tbody>
</table>
Appendix 3: Summary of HR functions with related risks and controls

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

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

Appendices
<table>
<thead>
<tr>
<th>HR function and risk</th>
<th>Risk type</th>
<th>System Control References</th>
<th>Manual Control References</th>
</tr>
</thead>
<tbody>
<tr>
<td>R408: Salary sacrifice arrangements are not appropriately managed.</td>
<td>$</td>
<td>S25</td>
<td>M62</td>
</tr>
<tr>
<td>R409: Methodology for bonus rewards is not established.</td>
<td>$</td>
<td>S26</td>
<td>-</td>
</tr>
<tr>
<td>R410: Employee benefits are not managed or administered in accordance with Workplace Agreements/employee contracts.</td>
<td>$</td>
<td>S27, S28</td>
<td>-</td>
</tr>
<tr>
<td><strong>System maintenance and integration</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R501: Payroll system does not reconcile to the General Ledger.</td>
<td>$</td>
<td>S29</td>
<td>M63</td>
</tr>
<tr>
<td>R502: Incomplete or inaccurate submission of superannuation data.</td>
<td>$</td>
<td>S30, S31</td>
<td>-</td>
</tr>
<tr>
<td>R503: Leave accrual rates are established inaccurately.</td>
<td>$</td>
<td>S32, S33</td>
<td>M64</td>
</tr>
<tr>
<td>R504: Employee wages paid in foreign currency are calculated incorrectly.</td>
<td>$</td>
<td>S34</td>
<td>-</td>
</tr>
<tr>
<td>R505: The HR system organisational chart does not accurately reflect current employees and their positions.</td>
<td>$</td>
<td>S35, S36, S37</td>
<td>-</td>
</tr>
<tr>
<td>R506: Payroll schemas are established or modified incorrectly or without authorisation.</td>
<td>$</td>
<td>S38</td>
<td>-</td>
</tr>
<tr>
<td>R507: Application is vulnerable to security and availability threats.</td>
<td>$</td>
<td>S39</td>
<td>M65</td>
</tr>
</tbody>
</table>
Table 5: Summary of system controls

<table>
<thead>
<tr>
<th>Ref</th>
<th>Control description</th>
<th>HR function</th>
<th>Risk Ref</th>
</tr>
</thead>
<tbody>
<tr>
<td>S01</td>
<td>Define key data entry fields.</td>
<td>HR and payroll data management</td>
<td>R201</td>
</tr>
<tr>
<td>S02</td>
<td>Restricting user access to view, establish and amend master data.</td>
<td>HR and payroll data management</td>
<td>R201</td>
</tr>
<tr>
<td>S03</td>
<td>Validation checks on certain fields warn the user that the information is duplicated in another employee record.</td>
<td>HR and payroll data management</td>
<td>R201</td>
</tr>
<tr>
<td>S04</td>
<td>Access to HR master data is appropriately configured and managed.</td>
<td>HR and payroll data management</td>
<td>R202</td>
</tr>
<tr>
<td>S05</td>
<td>Access to add an employee should be restricted to appropriate individuals and segregated from payroll maintenance.</td>
<td>Employee commencements</td>
<td>R301</td>
</tr>
<tr>
<td>S06</td>
<td>Application will warn user if termination date in the past is entered.</td>
<td>Employee exits and terminations</td>
<td>R302</td>
</tr>
<tr>
<td>S07</td>
<td>Workflow operates to require independent approval verification of termination date entered.</td>
<td>Employee exits and terminations</td>
<td>R302</td>
</tr>
<tr>
<td>S08</td>
<td>Application automatically calculates payment based on master data, termination date entered, and leave entitlements.</td>
<td>Employee exits and terminations</td>
<td>R302</td>
</tr>
<tr>
<td>S09</td>
<td>Application automatically changes status of employee to ‘terminated’ as at termination date entered.</td>
<td>Employee exits and terminations</td>
<td>R303</td>
</tr>
<tr>
<td>S10</td>
<td>Application automatically disables terminated employee’s access to SAP application based on termination date entered.</td>
<td>Employee exits and terminations</td>
<td>R303</td>
</tr>
<tr>
<td>S11</td>
<td>Application does not allow payment to be disbursed to employees with ‘terminated’ status.</td>
<td>Employee exits and terminations</td>
<td>R303</td>
</tr>
<tr>
<td>S12</td>
<td>Workflow approval of employee time.</td>
<td>Time reporting</td>
<td>R401</td>
</tr>
<tr>
<td>S13</td>
<td>System validation of time data entered.</td>
<td>Time reporting</td>
<td>R401</td>
</tr>
<tr>
<td>S14</td>
<td>Timesheets are locked for editing after submission.</td>
<td>Time reporting</td>
<td>R401</td>
</tr>
<tr>
<td>S15</td>
<td>Automated notifications.</td>
<td>Time reporting</td>
<td>R401</td>
</tr>
<tr>
<td>S16</td>
<td>Automated checks on leave applications to ensure sufficient entitlement.</td>
<td>Time reporting</td>
<td>R402</td>
</tr>
<tr>
<td>S17</td>
<td>Workflow approval of leave requests.</td>
<td>Time reporting</td>
<td>R402</td>
</tr>
<tr>
<td>S18</td>
<td>Restrict user access to amend work rosters.</td>
<td>Time reporting</td>
<td>R403</td>
</tr>
<tr>
<td>S19</td>
<td>Restrict user access to process prior period adjustment.</td>
<td>Time reporting</td>
<td>R404</td>
</tr>
<tr>
<td>S20</td>
<td>Workflow approval of prior period adjustments.</td>
<td>Time reporting</td>
<td>R404</td>
</tr>
<tr>
<td>S21</td>
<td>Limit prior period adjustments.</td>
<td>Time reporting</td>
<td>R404</td>
</tr>
<tr>
<td>S22</td>
<td>Restrict changes and user access to modify payroll calculation rules.</td>
<td>Payroll processing and administration</td>
<td>R405</td>
</tr>
<tr>
<td>S23</td>
<td>Restricted access to establish and amend taxation reference tables.</td>
<td>Payroll processing and administration</td>
<td>R406</td>
</tr>
<tr>
<td>Ref</td>
<td>Control description</td>
<td>HR function</td>
<td>Risk Ref</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>S24</td>
<td>Configure automated calculation of superannuation payable.</td>
<td>Payroll processing and administration</td>
<td>R407</td>
</tr>
<tr>
<td>S25</td>
<td>Salary sacrifice details are appropriately established in the HRMIS.</td>
<td>Payroll processing and administration</td>
<td>R408</td>
</tr>
<tr>
<td>S26</td>
<td>Utilise system functionality to accrue for and calculate bonus payments.</td>
<td>Payroll processing and administration</td>
<td>R409</td>
</tr>
<tr>
<td>S27</td>
<td>Correctly establish and manage employee benefits.</td>
<td>Payroll processing and administration</td>
<td>R410</td>
</tr>
<tr>
<td>S28</td>
<td>Restricted access to establish benefit plans.</td>
<td>Payroll processing and administration</td>
<td>R410</td>
</tr>
<tr>
<td>S29</td>
<td>Utilise auto-posting functionality.</td>
<td>Managing system interfaces</td>
<td>R501</td>
</tr>
<tr>
<td>S30</td>
<td>Superannuation data is provided in the required format and in the required timeframes.</td>
<td>Managing system interfaces</td>
<td>R502</td>
</tr>
<tr>
<td>S31</td>
<td>Changes to superannuation interfaces and data file formats are managed using entity IT change management controls.</td>
<td>Managing system interfaces</td>
<td>R502</td>
</tr>
<tr>
<td>S32</td>
<td>Manage leave accrual rules.</td>
<td>Managing system rules</td>
<td>R503</td>
</tr>
<tr>
<td>S33</td>
<td>Configuration of maximum values for leave accruals.</td>
<td>Managing system rules</td>
<td>R503</td>
</tr>
<tr>
<td>S34</td>
<td>Establish automated updates for foreign exchange rates.</td>
<td>Managing system rules</td>
<td>R504</td>
</tr>
<tr>
<td>S35</td>
<td>Restricted access to update organisational chart.</td>
<td>Managing system rules</td>
<td>R505</td>
</tr>
<tr>
<td>S36</td>
<td>Ability to display temporary assignments.</td>
<td>Managing system rules</td>
<td>R505</td>
</tr>
<tr>
<td>S37</td>
<td>Organisational chart designed to reflect the hierarchy.</td>
<td>Managing system rules</td>
<td>R505</td>
</tr>
<tr>
<td>S38</td>
<td>Access to establish or modify payroll schemas or elements and rules is restricted.</td>
<td>Managing system rules</td>
<td>R506</td>
</tr>
<tr>
<td>S39</td>
<td>Automatic notification of available software updates.</td>
<td>Managing software updates</td>
<td>R507</td>
</tr>
</tbody>
</table>
Appendix 4: PeopleSoft and SAP HRMIS functionality

The PeopleSoft and SAP HRMIS applications are used by a number of Australian Government entities to manage HR and payroll functions. There are many controls available within each of these applications which can assist in the mitigation of key payroll and HR risks. Implementation of automated controls may reduce the current effort associated with performance of manual controls, designed to achieve the same objective.

The Online Supplement of this Guide available electronically from the ANAO website provides further detail on security controls, segregation of duty considerations and useful reports for these two systems.

Functional overview of Oracle PeopleSoft Enterprise Release 8.0 Human Resources module

Functionality in PeopleSoft Human resources module has four key areas that support HR management functions and is illustrated in the diagram below:

Figure 4: Oracle PeopleSoft HR module functionality

<table>
<thead>
<tr>
<th>Global core HCM</th>
<th>This module provides functionality management of benefits Administration and Payroll for organisations that manage a workforce globally and are required to comply with local laws and regulations for management of deductions and other HR functions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workforce Administration</td>
<td>This module supports workforce administration and assists with management of absences, resources allocation and position management, travel and expense management.</td>
</tr>
<tr>
<td>Workforce Service Delivery</td>
<td>This module supports HR management functions, such as HR Helpdesk functions and supports employee self-service functionality for benefits and pay reporting.</td>
</tr>
<tr>
<td>Integrated Talent Management</td>
<td>This module supports an organisation’s learning and development framework and staff performance management.</td>
</tr>
</tbody>
</table>

PeopleSoft security

Security implementation in a large and complex system such as the PeopleSoft application requires an understanding of the security structure. This section of the Online Supplement provides a high-level overview of PeopleSoft security and discusses:

- User security;
- Using internet protocols to access the PeopleSoft application;
- Authentication and single sign-on; and
- Data permission security.
The following diagram illustrates, at a high level, the PeopleSoft security model.

**Figure 5: PeopleSoft Security**

---

**PeopleSoft security and administration**

The three main PeopleSoft security definition types are:

- **User Profiles** (a set of data describing a particular PeopleSoft user);
- **Roles** (intermediate objects that link User Profiles to Permission Lists); and
- **Permission Lists** (a set of pages and allowable actions on those pages).

Implementation of security in PeopleSoft requires security administrators to use a hierarchy to implement user security. The hierarchy is:

**Figure 6: PeopleSoft security hierarchy**

---

A **user profile** is a definition that represents a single PeopleSoft user. Each user is unique; the user profile specifies a number of user attributes, including one or more assigned roles. Each role that is assigned to a given user profile adds its permission lists to the total that applies to that user.

A **role** is a collection of permission lists. One or more permission lists can be assigned to a role. Similarly a given permission list can be assigned to multiple roles. The resulting combination of permissions can apply to all users who share those access requirements. The same group of users might also have other access requirements that they do not share with each other. Roles are used to assign permissions to users dynamically.

**Permission Lists** are the foundation of user security authorisation for the PeopleSoft application. A permission list grants a degree of access to a particular combination of PeopleSoft elements, specifying pages, development environments, time periods, and administrative tools, for example.
This level of access should be appropriate to a narrowly defined and limited set of tasks, which can apply to a variety of users with a variety of different roles. These users might have overlapping, but not identical, access requirements.

The diagram below illustrates the relationship between Users, Roles and Permission Lists. Permission lists are assigned to roles, which are then assigned to user profiles. A role may contain numerous permissions and a user profile may have numerous roles assigned to it. Because permission lists are applied to users through roles, a user inherits all the permissions assigned to each role to which the user belongs. The user’s access is determined by the combination of all of the roles.

**Figure 7: Users, Roles and Permission Lists**

**Using Internet protocols to manage access**

One alternative approach to implementing PeopleSoft security utilises Internet protocols to access a directory that is maintained by the IT or application security administrator. The alternative approach allows an organisation to typically store user profiles in a central repository that serves user information for all of the programs that require it.

**Authentication and single-sign on**

Single sign-on uses digital certificates to authenticate users and secure the transmission of data. Within the context of the PeopleSoft system, single sign-on means that after a user has been authenticated by one PeopleSoft application server, that user can access a second PeopleSoft application server without entering a user identifier or an additional password.

**Data permission security**

Maintaining the confidentiality of employee master data is critical. Data permission security works by associating an employee’s data with a department code. Using security trees, user access to data permission lists is provided to certain departments. This in turn, provides users with access to the respective employee information. Users are then assigned a data permission list. When a user accesses the system, their data permission lists identify which department’s employee data they can access.

**Segregation of duties considerations**

Segregation of duties in PeopleSoft is achieved by ensuring that user access to roles or to permission lists does not allow a user to perform conflicting functions.
SAP ECC 6.0 Human Capital Management module

A discussion of the functionality, risks and controls of the Human Resources module up to version ECC 6.0 is covered within the SAP ECC 6.0 Security and Control Better Practice Guide released in June 2009. This Guide provides further detail on risks and controls by HR function.

Figure 8: SAP Human Capital module

Prior to version 4.6, personnel management was split into two sub-modules known as Personnel Administration and Personnel Planning and Development. These modules were combined in version 4.6 and are now collectively known as Personnel Management.

The Personnel Management module is used for:
- Maintaining all employee and organisational master data;
- Processing employee hiring and termination;
- Performing organisational planning, budgeting, and recruitment; and
- Administering salaries, benefits, and expenses.

Personal Time Management
- This module is used in the planning, recording and valuation of employee work performed and absence times.

Payroll Accounting
- This module provides a number of work processes including the generation of payroll results and remuneration statements, bank transfers and cheque payments.

Employee Self Service (ESS)
- The self service module allows employees to maintain their time sheet, leave requests, personal information, and display of pay slips.

Managers Desktop
- This module allows functional managers to perform administrative tasks within their area and access relevant HR, financial, or controlling data.

SAP security

Readers should refer to the ECC 6.0 Security and Control Better Practice Guide published by the ANAO in June 2009 which contains significant detail and description on implementation of appropriate security controls and understanding the SAP security structure.

Transaction codes and authorisation objects

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

Segregation of duties considerations

In SAP terms, a segregation of duties’ risk occurs when user access is granted to an object that associates two or more conflicting functions. A function is a task that an employee performs to accomplish a specific portion of their job responsibilities.
Index

A

access controls
  data management 15–16, 20, 26
  defined 75
  organisational chart 67
  payroll processing 44–45, 50, 53
  PeopleSoft 88–89
  SAP 90
  systems 71
  workforce management 33, 36
accounting
  financial reporting interface 61
  leave accrual 65–66
  payroll 47–54, 59, 61–63
accumulated contribution schemes 48, 52
accuracy, of payroll calculations 41, 50, 67–68
audit report 75
‘audit’ tables 16
Australian Government ICT Security Manual (ISM) 6
Australian Government Protective Security Policy Framework 6, 14
Australian Public Service Commission (website) 82
Australian Taxation Office (website) 82
authentication, in PeopleSoft 89
authorisation
  amended timesheets 46
  leave requests 44, 46
  payment disbursal 54
  payroll schemas 67
  prior period adjustments 45
  self-service functions 56
authorisation objects 90
automated control. See system controls
auto-posting functionality 62

B

backup controls 20, 71
banking applications 54
benefits 48, 53, 54
Better Practice Guides (ANAO) 6. See also Human Resource Management Information Systems guide
Blueprint for the Reform of Australian Government Administration 3
bonus payments 49, 52, 54
business continuity management 71

C

change management process
  defined 75
  self-service functionality 56
  system maintenance 70
clean desk policy 16
Commonwealth Authorities and Companies Act 1997 (Cth) 60, 81
Commonwealth Fraud Control Guidelines 2002 (Cth) 79
Commonwealth Procurement Guidelines (CPGs) 60, 81
Commonwealth Superannuation Scheme (CSS) 49
completeness, of payroll processing 41, 50
compliance
  data management 6, 14, 21
  payroll processing 42, 51, 53
  system maintenance and integration 60
  workforce management 31, 34
compliance risk 8
ComSuper (website) 82
ComSuper interface 59, 61
configuration
  defined 9, 75
  payroll 64, 68, 70
configuration control 75. See also system controls
configuration reports 16, 33
control objectives
  data management 14
  defined 7, 75
  payroll processing 41
  system maintenance and integration 59
  workforce management 31
controls 7–8
  data management 15–16, 83
  defined 75
  identifying 9
  manual (See manual controls)
  payroll processing 43–46, 48, 50–54, 83–84
  software updates 69
  summary of 83–86
  system (See system controls)
  system interfaces 62–63, 70
  system maintenance and integration 59, 84
  system rules management 66–68
  workforce management 33–37, 83
  cost centre 36, 75
  customisation 9, 75
D

data
defined 75
master (See master data)
reference 13
database(s)
defined 75
change management and 70
software updates 69
system rules and 64
data management 5, 6, 11–27
classification 13
compliance issues 6, 14, 21
control objectives 14
employee commencement 32–34
privacy practices 14, 17–27
risks and controls 15–16, 83
data permission security 89
data transfer 61
deductions, payroll 48, 52
default 75
defined benefit schemes 49, 52
Department of Education, Employment and Workplace Relations (website) 82
Department of Finance and Deregulation (website) 82
digital certificates 89
duplicate employees 33, 75

E

edit access 16, 75
Electronic Funds Transfer (EFT) 54
employee(s). See also workforce management
benefits 48, 53, 54
bonus payments 49, 52, 54
duplicate 33, 75
exits and terminations 33, 35–37
information (See data management)
leave (See leave accrual)
new 32–34
payments (See payroll payment)
promotions 32
self-service functionality for 55–56
superannuation (See superannuation)
time reporting 43–45
transfers 32–34
Employee Changes Reports 50
employee contribution 48, 75

Employee Exit checklist 36
Employee Self Service (ESS) 55–56, 75
employer contribution 48, 51
Enterprise Resource Planning (ERP) systems 61
exit process 33, 35–37

F

Fair Work Act 2009 (Cth) 79
field
defined 75
key data 15, 33
Finance Minister’s Orders for Financial Reporting 60, 81
Financial Management and Accountability Act 1997 (Cth) 60, 81
Financial Management and Accountability Regulations 1997 (Cth) 31, 34, 60, 80, 81
financial reporting interface 61
financial risk 8
foreign exchange rate (FX) 59, 65, 66, 68
fraud risk 8
Freedom of Information Act 1982 (Cth) 21
Fringe Benefits Tax (FBT) 48, 50
function, defined 76, 90

G

General Ledger, posting to. See posting
Gershon Review 3, 9
'ghost' (non-existent) employees 33
Global Payroll Tables (PeopleSoft) 64

H

higher duties 32
human resource (HR) functions 5–8
summary of 83–84
data (See data management)
payroll (See payroll processing and administration)
systems (See system maintenance and integration)
workforce (See workforce management)
Human Resource Management Information Systems (HRMIS), defined 76
central themes in 6–8
legislation list 80–81
Online Supplement 4, 6, 64, 87
purpose of 3
structure of 4
human resource (HR) risks. See risk(s)
Human Resources Tables (PeopleSoft) 64
I

Information and Communication Technology (ICT) systems 6
Information Privacy Principles 6, 14
1 (manner and purpose of collection) 18, 24
2 (solicitation individually) 18–19, 24
3 (solicitation generally) 19, 24
4 (storage and security) 20, 25
5 (record-keeping) 21, 25
6 (access to records) 21, 26
7 (alteration of records) 22, 26
8 (accuracy checks) 22, 26
9 (relevant use) 22, 26
10 (limits on use) 23, 27
11 (disclosure limits) 23, 27
employee commencement and 32, 34
summary of 17
information systems, information exchange between 61
Information Technology (IT) initiatives 3
integrated systems 61
integrity
defined 76
of information 3, 6, 70
system interfaces and 61–62
inter-agency transfers 33, 34
interface
defined 76
financial reporting 61
interface management 61–63, 70
internal control
effectiveness of 5
segregation of duties and 7
Internet protocols 89

L
leave accrual
accounting for 65–66
control objectives 59, 68
time reporting and 44, 46
legislation. See also specific law
data management 6, 14
of general relevance 79
payroll processing 42, 51
referred to in Guide 80–81
system maintenance and integration 60
workforce management 31
logical access 76
long service leave 65
Long Service Leave (Commonwealth Employees) Act 1976 (Cth) 42, 80

M
management controls, over payroll configuration 68, 70
Manager Self Service (MSS) 76
manual controls 7–8
data management 15–16
payroll processing 43–44, 48, 50–53
software updates 69
summary of 83–84
system interfaces 62
system rules 66
workforce management 33, 35–36
manual journal 49
master data
defined 13, 76
managing 15–16
system controls 20
Maternity Leave (Commonwealth Employees) Act 1973 (Cth) 42, 80
'Missing Time' report 43
module(s)
defined 76
PeopleSoft 87
SAP 90

N
National Privacy Principles 17
new employees 32–34
notifications
software updates 69
time reporting 43

O
Office of the Australian Information Commissioner (website) 82
one-off payment 35
Online Supplement (HRMIS guide) 4, 6, 64, 87
Oracle PeopleSoft
defined 76
functional overview of 87–89
Online Supplement detail on 4, 6, 87
payroll configuration 64
website 82
organisational structures 65, 67–68

P
parameters
defined 76
setting of (See configuration)
PAYG (Pay As You Go)
payroll deductions 48, 50
payments
  bonus 49, 52, 54
  one-off 35
  payroll (See payroll payment)
  termination 35
Payroll Budget to Variance Reports 50
payroll calculation
  accuracy of 41, 50, 64
  approval of 47
  control framework 5, 34
  defined 76
  leave accruals and 66
  superannuation in 48, 51
payroll configuration 64, 68, 70
payroll data management. See data management
payroll exception reporting 49, 76
Payroll Exception Reports 50
Payroll Interface File format 61
payroll journal 59, 61
payroll payment
  by electronic funds transfer 54
  function 47
payroll processing and administration 5, 39–56
  accounting 47–54, 59, 61–63
  compliance issues 42, 51, 53
  control objectives 41
  overview of 47
  risks and controls 43–46, 48, 50–54, 83–84
  self-service functionality 55–56
  system maintenance and integration 59, 64–68
  time reporting 43–45
pay run processing 47, 54
PeopleSoft. See Oracle PeopleSoft
periodic review
  of foreign currency payments 68
  of organisational chart 68
permanent transfer 32
Permission Lists (PeopleSoft) 88–89
personal information
  access to 21, 26
  accuracy checks 22, 26
  alteration of 22, 26
  defined 18
  disclosure limits 23, 27
  limits on use of 23, 27
  manner and purpose of collection 18, 24
  record-keeping 21, 25
  relevant use of 22
  solicitation of 18–19, 24
  storage and security of 20, 25
physical access
  defined 76
  employee termination and 35
policy development, payroll processing 54
position-based security
  defined 77
  employee termination and 36
position management 32, 59, 65, 67
posting
  of leave accrual 65
  of payroll expenses 59, 61, 62–63
preventive controls 9
prior period adjustments
  defined 77
  in time reporting 45
Privacy Act 1988 (Cth) 17, 18, 79
Privacy Obligations for Commonwealth Contracts 17
privacy officer 21
privacy practices 6
  data management 14, 17–27
  workforce management 33, 34
profile(s)
  access based on 16
  defined 77
  in organisational structure 16
  PeopleSoft 88–89
promotions 32
protection of information risk 8
Public Sector Accumulation Plan (PSSAP) 48, 49
Public Service Act 1999 (Cth) 31, 80
Public Service Classification Rules 2000 (Cth) 31, 80
Public Service Commissioners Directions 1999 (Cth) 31, 80
Public Service Regulations 1999 (Cth) 31, 80
R
reconciliation
  defined 77
  payroll payments 48, 54, 62–63
  terminations 37
record-keeping 21
reference checking policy 34
reference data 13
references, external 82
relevant controls 9
reporting risk 8
Index

risk(s)  5, 7
  data management  14–16, 83
defined  77
  payroll processing  43–45, 50–53, 83–84
  software updates  69
  summary of  83–84
system interfaces  62
system maintenance and integration  59, 84
  system rules  66–67
  types and classifications  8
  workforce management  33, 35, 83
role(s)
  access based on  15–16, 51, 53, 71
defined  77
  PeopleSoft  88–89
  position management  32, 65
rules management (system)  64–68

S
Safety Rehabilitation and Compensation Act 1988 (Cth)  42, 80
salary sacrifice  49, 51, 54
SAP
  defined  77
  functional overview of  90
  Online Supplement detail on  4, 6, 87
  payroll configuration  64
  website  82
schema
  payroll  59, 64, 67–68
security
  data  14, 16, 20, 25, 89
  ICT systems  6
  PeopleSoft  87–88
  position-based  36, 77
  SAP  90
  self-service functionality  56
  system maintenance and integration  59
security clearance, for new employees  34
segregation of duties (SOD)
  control mechanisms for  7, 9
  for data management  16
defined  77
  for payroll processing  51
  in PeopleSoft  89
  in SAP  90
  for systems management  70–71
segregation of duties conflict  77, 90
self-service functionality  55–56
Service Level Agreement (SLA)  77
single sign on (SSO)
defined  77
  in PeopleSoft  89
  terminations and  36
software updates
defined  76
  management of  69, 70
storage
  of documentation  16
  of personal information  20
  system maintenance and  71
superannuation
  accumulated contribution schemes  48, 52
  data submission  59, 61–62
defined benefit schemes  49, 52
  legislative requirements  48, 51
  salary sacrifice  49, 51, 54
  Superannuation Act 1976 (Cth)  42, 80
  Superannuation Act 1990 (Cth)  42, 80
  Superannuation Act 2005 (Cth)  42, 81
  Superannuation (Productivity Benefit) Act 1988 (Cth)  42, 80
  Superannuation Guarantee (Administration) Act 1992 (Cth)  42, 48, 81
system controls  7
  data management  15–16, 20
defined  77
  payroll processing  43–44, 48, 50–53
  software updates  69
  summary of  83–86
  system interfaces  62
  system rules  66–67
  workforce management  33, 35–36
system maintenance and integration  5, 57–71
  compliance issues  60
  control objectives  59
  interface management  61, 70
  risks and controls  59, 84
  rules management  64–68
  software updates  69, 70
system reports
  configuration  16, 33
  data management  16
  payroll processing  49, 50
  workforce management  33, 36
Managing Human Resource Information Systems – Risks and Controls

Better Practice Guide

T

Table(s)
- 'audit' 16
- defined 77
- in Oracle PeopleSoft 64
- taxation (See taxation tables)
- taxation 48, 50, 52
- Taxation Administration Act 1953 (Cth) 42, 81
- Taxation Administration Regulations 1976 (Cth) 42, 81
- taxation tables
  - access controls 50
  - automated updates 52
  - data type 13
- template forms
  - leave requests 46
  - new hire 34
- temporary assignments 67
- temporary transfer 32
- terminations 33, 35–37
- test environment 70, 78
- time reporting 43–45
- timesheets 43, 46
- total remuneration packaging (salary sacrifice) 49, 51, 54
- transaction codes
  - defined 78
  - SAP 90
- transfers
  - data 61
  - employee 32–34

W

Website(s), external references 82
- workflow
  - defined 78
  - self-service functionality and 55, 67
  - termination date approvals 35
  - time reporting approvals 43–45
- workforce management 5, 29–37. See also employee(s)
  - compliance issues 31, 34
  - control objectives 31
  - risks and controls 33–37, 83
  - system maintenance and integration 59
  - working time, reporting of 43–45
- work rosters 43, 44

U

User acceptance testing 56, 70
- user access control. See access controls
- user profiles. See profile(s)

V

Validation checks
- data management 15, 20
- defined 78
- foreign exchange rates 68
- payroll processing 43, 49
- workforce management 33, 35, 37
- view access 78