



# Prudential Practice Guide

## **PPG 234 – Management of security risk in information and information technology**

1 February 2010

## Disclaimer and copyright

This prudential practice guide is not legal advice and users are encouraged to obtain professional advice about the application of any legislation or prudential standard relevant to their particular circumstances and to exercise their own skill and care in relation to any material contained in this guide.

APRA disclaims any liability for any loss or damage arising out of any use of this prudential practice guide.

© Commonwealth of Australia

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. All other rights are reserved.

Requests and inquiries concerning reproduction and rights should be addressed to:

Commonwealth Copyright Administration  
Copyright Law Branch  
Attorney-General's Department  
Robert Garran Offices  
National Circuit  
Barton ACT 2600  
Fax: (02) 6250 5989

or submitted via the copyright request form on the website <http://www.ag.gov.au/cca>

## About this guide

This prudential practice guide (PPG) aims to assist regulated institutions in the management of security risk in information and information technology (IT). It is designed to provide guidance to senior management, risk management and IT security specialists (management and operational).

The PPG targets areas where APRA continues to identify weaknesses as part of its ongoing supervisory activities. The PPG does not seek to provide an all-encompassing framework, or to replace or endorse existing industry standards and guidelines.

Subject to meeting APRA's prudential requirements, regulated institutions have the flexibility to manage security risk in IT in a manner best suited to achieving their business objectives. Not all of the practices outlined in this prudential practice guide will be relevant for every regulated institution and some aspects may vary depending upon the size, complexity and risk profile of the institution.

# Contents

<b>Introduction</b>	<b>6</b>
<b>IT security risk</b>	<b>7</b>
Definition	7
Risk management	8
Classification by criticality and sensitivity	8
Industry baselines	8
<b>An overarching framework</b>	<b>9</b>
Hierarchy of policies, standards, guidelines and procedures	9
A principles-based approach	9
Policy domains	10
Ongoing compliance	10
Ongoing assessment of effectiveness	11
<b>User awareness</b>	<b>11</b>
Training and awareness programs	11
User education areas	11
User compliance	12
<b>Access Control</b>	<b>12</b>
Access based on business need	12
Identification and authentication techniques	12
Access control techniques	12
Data/information leakage	13
Cryptographic techniques to restrict access	14
<b>IT asset life-cycle management controls</b>	<b>14</b>
IT security considered at all stages	14
Physical security	15
Secure software development	15
IT security technology solutions	15
End-user developed/configured software	15
Legacy technologies	16
Emerging technologies	16

<b>Monitoring and incident management</b>	<b>16</b>
Monitoring processes	16
Incident management	17
Accountability and audit trails	17
<b>IT security reporting and metrics</b>	<b>17</b>
Regular reporting	17
Effective IT security metrics	18
<b>IT security assurance</b>	<b>18</b>
Assurance program	18
Frequency of assurance	18
Independence	18
<b>Attachment A: Change management</b>	<b>19</b>
<b>Attachment B: Resilience and recovery</b>	<b>20</b>
<b>Attachment C: Service provider management</b>	<b>23</b>
<b>Attachment D: Secure software development</b>	<b>24</b>
<b>Attachment E: Customer protection</b>	<b>26</b>
<b>Attachment F: Cryptographic techniques</b>	<b>27</b>

## Introduction

1. Continued developments in information<sup>1</sup> and information technology (IT)<sup>2</sup> have brought about an increased reliance by financial service organisations on IT assets<sup>3</sup>, including software, hardware and data/information (both soft and hard copy). Consequently, stakeholders including Boards of Directors (Boards), senior management, shareholders, customers and regulators have heightened expectations regarding the effective safeguarding of IT assets. For ease of reference, the term 'IT' in this document relates to both information and information technology.
2. This prudential practice guide (PPG) targets areas where IT security risk management weaknesses continue to be identified as part of APRA's ongoing supervision activities. While the PPG provides guidance for safeguarding IT assets, it does not seek to be an all-encompassing framework. APRA expects that regulated institutions, using a risk-based approach, will implement appropriate controls for IT assets even in areas not addressed by this PPG.
3. This PPG aims to provide guidance to senior management, risk management and IT security specialists (management and operational) in APRA-regulated institutions. The multiple audiences reflect the pervasive nature of IT security risk management, and the need for sound risk management disciplines and solid business understanding to evaluate and manage the IT security risk profile. Additionally, effective IT security risk management can facilitate business initiatives and assist compliance with other regulatory requirements (e.g. privacy and anti-money laundering).
4. As with any process, governance is vital to ensure that risk management processes are properly designed and operating effectively to meet the needs of the institution. In APRA's view, effective governance of IT security risk management would be aligned to the broader IT and corporate governance frameworks and involve the clear articulation of Board and senior management responsibilities and expectations, formally delegated powers of authority, and regular oversight.
5. Subject to APRA's prudential standards, an APRA-regulated institution has the flexibility to manage IT security risks in the way most suited to achieving its business objectives. Where the content of this PPG touches on matters contained in the prudential standards, the intent is to provide guidance where the standards relate to IT security risk management.
6. This PPG does not seek to replace or endorse existing industry standards and guidelines. A regulated institution would typically use discretion in adopting whichever industry standards it sees fit for purpose in specific control areas. In addition, the level, scope and language used within this PPG reflect a broader target audience, coming from a variety of disciplines and levels within an organisation. In APRA's view, useful guidance may also be obtained from industry-accepted standards such as COBIT<sup>4</sup>, ISO standards<sup>5</sup>, Standards Australia<sup>6</sup> and ITIL<sup>7</sup> in that they provide broad frameworks for establishing and maintaining control environments.

1 Information is the result of processing, manipulating and organising data.

2 Computer-based technology comprising software, hardware and data.

3 Anything deemed to be of value (either financial or otherwise) by an organisation, pertaining to IT.

4 Control Objectives for Information and related Technology (COBIT) issued by the Information Systems Audit and Control Association (US-based).

5 As issued by the International Organization for Standardization (ISO), an international standards-setting body headquartered in Switzerland.

6 A non-government Australian-based standards development body.

7 IT Infrastructure Library (ITIL) issued by the Office of Government Commerce (UK-based).

7. The relevance of the content of this PPG will be different for each institution and will vary depending upon factors such as the nature, size, complexity, risk profile and risk appetite of the institution. In a number of areas, the PPG provides sample practices to illustrate a range of controls that could be deployed to address a stated principle. These samples are not intended to be exhaustive compliance checklists.
8. Included within the PPG are a number of attachments. These have been created in areas where APRA has identified that more detailed and technical guidance is necessary.

## IT security risk

### Definition

9. IT security risk represents the intersection of IT risk and security risk which, in turn, are subsets of operational risk (see diagram below).



10. For the purposes of this PPG, security risk is defined as the potential compromise of an asset's:
  - (a) confidentiality: only authorised access permitted;
  - (b) integrity: completeness, accuracy and freedom from unauthorised change; or
  - (c) availability: accessibility and usability when required.

Attributes such as accountability<sup>8</sup>, authenticity<sup>9</sup>, and non-repudiation<sup>10</sup>, while they do not define security, are important security considerations.

11. A compromise of one or more of these attributes can have a detrimental impact on a regulated institution and could result in a failure to meet its business objectives (including regulatory and prudential requirements).
12. IT risk encompasses the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events impacting on IT assets, and would be managed in alignment with the operational risk framework<sup>11</sup>. This includes IT assets managed and developed/ supported by a dedicated technology function, service providers and/or teams/individuals<sup>12</sup> located within business units<sup>13</sup>.
13. IT security risk, therefore, can be described as the risk of loss due to inadequate or failed internal processes, people and systems or from external events, resulting in a compromise of an IT asset's confidentiality, integrity or availability.

<sup>8</sup> The ability to attribute the responsibility for an action.

<sup>9</sup> The quality or condition of being genuine.

<sup>10</sup> The concept that an event cannot later be denied.

<sup>11</sup> Including the identification, assessment, management and monitoring of risk.

<sup>12</sup> This includes end-user developed/configured software.

<sup>13</sup> Some regulated institutions may choose a broader definition of IT risk to include, for example, opportunity cost to obtain business advantage, efficiency or effectiveness.

## Risk management

14. In APRA's view, IT security risk (as with the broader set of IT risks) will ultimately result in a business risk exposure. Regulated institutions would benefit from clearly defining both IT risk and IT security risk. In addition, allocation mechanisms would typically be developed for mapping these risks to business risks, based on relevant risk categorisations, enabling allocation of individual and aggregate risks to those accountable for ownership, management and control of risk. This includes the ability to assess these risks both within and across business units, including at the enterprise level<sup>14</sup>.
15. Regulated institutions have developed distinct practices and disciplines to manage IT security risks, IT risks and operational risks. In APRA's view, these are all necessary and complementary disciplines.
16. An important goal of IT security risk management (as with the broader set of IT risks) is to ensure that the business objectives of the institution continue to be met. It is important that an individual business unit's objectives are not considered in isolation but rather in the context of the objectives of the institution as a whole.
17. In APRA's view, IT risk exposures that could have a material impact on a regulated institution would typically be controlled/mitigated to a level that ensures the institution's ability to meet regulatory and prudential requirements or operate as a going concern is not compromised by an incident<sup>15</sup>.

18. The adequacy of IT security controls in ensuring that a regulated institution remains within its risk appetite would normally be assessed on a regular basis (or following material change to either the internal control or external environments). The assessment would typically take into account the end-to-end control environment (including mitigating controls). Changes to the control environment would follow normal business case practices, taking into account the likelihood and impact of an event against the cost of the control.
19. The IT security risk management process is a continuous and dynamic process that ensures emerging IT vulnerabilities/threats<sup>16</sup> are identified, assessed and appropriately managed<sup>17</sup> in a timely manner.

## Classification by criticality and sensitivity

20. For the purposes of managing IT risk, a regulated institution would typically classify IT assets based on business criticality and sensitivity. Institutions may seek to leverage the existing business impact analysis process to achieve this. The institution's IT asset classification method and granularity would normally be determined by the requirements of the business.

## Industry baselines

21. A regulated institution could find it useful to regularly assess the completeness of its IT security risk management framework by comparison to peers and established control frameworks and standards.

14 The ability to aggregate and assess risks at the enterprise (whole-of-business) level is an important component of the identification and management of emerging and growing risks.

15 For the purposes of this PPG, incidents are any events that potentially compromise the confidentiality, integrity and availability of IT assets.

16 Threats relate to the potential compromise of IT assets through the exploitation of vulnerabilities.

17 Alternative ways of managing include mitigation, termination, transfer or acceptance of the risk exposure.

## An overarching framework

### Hierarchy of policies, standards, guidelines and procedures

22. An IT security risk management framework outlines a regulated institution's approach to managing IT security and is typically embodied in a hierarchy of policies, standards, guidelines and procedures. It would typically align to other enterprise frameworks such as project management, outsourcing management and risk management.
23. The IT security risk management framework would typically enable the design and implementation of the IT security controls. The strength of controls would normally be commensurate with the criticality and sensitivity of the IT asset involved.
24. The establishment and ongoing development of the IT security risk management framework would normally be directed by an overarching IT security strategy and a supporting program of work. This strategy would typically be aligned with a regulated institution's IT and business strategies, as appropriate.
25. In APRA's view, the IT security risk management framework would encapsulate the expectations of the Board and senior management, have a designated owner(s), and outline the roles and responsibilities of staff to ensure the achievement of effective IT security risk management outcomes. The framework would be formally approved and reviewed on a regular basis, with periodic assessment for completeness against current practices and industry standards.

### A principles-based approach

26. APRA envisages that a regulated institution would adopt a set of high-level IT security principles in order to establish a sound foundation for the IT security risk management framework. Common IT security principles include:
  - (a) defence-in-depth and diversity of controls, where multiple layers and types of controls are used to address risks in different ways. Therefore, should one control layer be compromised, other control(s) limit the impact on a regulated institution;
  - (b) denial of all features, permissions, functions and protocols unless required to conduct business operations. This reduces the number of attack approaches that may be used to compromise IT assets;
  - (c) timely detection and reporting of IT security breaches. This minimises the time in which a compromise of an IT asset can impact on a regulated institution;
  - (d) appropriately controlled error handling. Errors should not allow unauthorised access to IT assets or other IT security compromises;
  - (e) distrust of unfamiliar IT assets, including internal and external IT assets. Such assets have an unknown and possibly reduced level of IT security control;
  - (f) segregation of duties, enforced through appropriate allocation of roles and responsibilities. This reduces the potential for the actions of one person to compromise IT assets; and
  - (g) a control environment designed to enforce compliance rather than assume staff are fully familiar with IT security policies and procedures.

## Policy domains

27. Sound practice would be to establish policies with supporting standards, guidelines and procedures in the following areas, with higher level policies normally linked to desired business outcomes. A policy framework would normally take into consideration:

- (a) identification, authorisation and granting of access to IT assets (by individuals and other IT assets);
- (b) definition of an overarching IT security architecture that outlines the direction for the design of the IT environment (encompassing all IT assets) from a security perspective (e.g. network zones/segments, gateway design, authentication, identity management, message routing, software engineering and location of IT security technology solutions);
- (c) life-cycle management that addresses the various stages of an IT asset's life to ensure that IT security requirements are considered at each stage. This includes configuration standards;
- (d) management of IT security technology solutions that include firewall, anti-malicious software, intrusion detection/prevention, cryptographic systems and monitoring/log analysis tools;
- (e) monitoring and incident management to address the identification and classification of incidents, reporting and escalation guidelines, preservation of evidence and the investigation process;
- (f) management and monitoring of service providers that defines the framework for overseeing the management of IT security risks by third parties;

- (g) acceptable usage of IT assets that defines the IT security responsibilities of users (staff, service providers and customers) in the use of IT assets;
- (h) recruitment and selection of IT staff and contractors that defines the framework for vetting and monitoring of personnel, taking into account IT security risk; and
- (i) IT security roles and responsibilities that may include:
  - (i) IT security risk management framework roles: maintenance, ongoing review, compliance monitoring, training and awareness;
  - (ii) IT security-specific roles<sup>18</sup>: IT security manager/officer, administrators, specialists;
  - (iii) IT asset-specific roles: owners<sup>19</sup>, custodians, end-users;
  - (iv) risk management, assurance and compliance roles; and
  - (v) formally constituted IT governance functions and reporting mechanisms to assess the ongoing effectiveness of the IT security risk management framework.

## Ongoing compliance

28. A regulated institution would normally implement processes that ensure compliance with regulatory and prudential requirements and the internal IT security risk management framework. APRA envisages that this would include ongoing checks by the compliance function (or equivalent), supported by reporting mechanisms (e.g. metrics, exceptions) and management reviews.

<sup>18</sup> Roles and responsibilities should not compromise appropriate segregation of duties (e.g. separation of security operations from policy setting and monitoring functions).

<sup>19</sup> In APRA's view, IT asset owners are important in determining the level of acceptable residual risk.

29. A regulated institution would normally implement an exemption policy for handling instances of non-compliance with the IT security risk management framework including: management of the exemption register; authority for granting exemptions; expiry of exemptions; and the review of exemptions granted. Where exemptions are granted, APRA envisages that an institution would review and assess the adequacy of compensating controls initially and on an ongoing basis. Compensating controls would normally reduce the residual risk in line with the institution's risk appetite.

### **Ongoing assessment of effectiveness**

30. APRA envisages that a regulated institution would regularly assess IT security vulnerabilities and evaluate the effectiveness of the existing IT security risk management framework, making any necessary adjustments to ensure emerging vulnerabilities are treated in a timely manner. This assessment would normally also be conducted as part of any material change.
31. A regulated institution would normally manage the initial development and continuing updates to the IT security risk management framework as an ongoing program of work. Subject to the materiality of changes to the IT security risk management framework, the body of work would typically be managed as a formal project with a clearly defined budget, resource requirements, timeframes and milestones, or using business-as-usual processes.
32. APRA envisages that control gaps identified in the IT security risk management framework would be addressed in a systematic way. This may involve the formulation of an IT security program that specifies target IT security metrics, timeframes for resolution and associated action plans for closing the gaps. Typically, action plans would be prioritised and tracked.

## **User awareness**

### **Training and awareness programs**

33. A regulated institution could benefit from developing an initial, and ongoing, training and IT security awareness program. This would typically incorporate any changes in IT security vulnerabilities or the institution's IT security risk management framework. Sound practice would involve the tracking of training undertaken and the testing of staff understanding as to the relevant IT security policies (both on commencement and periodically).

### **User education areas**

34. A regulated institution would regularly educate users as to their responsibilities regarding securing IT assets. Common areas covered would normally include:
- (a) personal versus corporate use of IT assets;
  - (b) email usage, internet usage (including social networking) and malware protection;
  - (c) physical protection, remote computing and usage of mobile devices;
  - (d) access controls including standards relating to passwords and other authentication requirements;
  - (e) responsibilities with respect to any end-user developed/configured software (including spreadsheets, databases and office automation);
  - (f) handling of sensitive data/information; and
  - (g) reporting of IT security incidents and concerns.
35. In the case of remote computing, a regulated institution would normally make users aware of the increased IT security threats, particularly with respect to unprotected environments.

## User compliance

36. A regulated institution would typically require users to adhere to appropriate IT security policies pertinent to their roles and responsibilities. As a minimum, all users would typically be required to periodically sign-off on these policies as part of the terms and conditions of employment or contractual agreements.

## Access Control

### Access based on business need

37. A key requirement for ensuring IT security is an effective process for providing access to IT assets. A regulated institution would normally only authorise access to IT assets where a valid business need exists and only for as long as access is required.
38. Factors to consider when authorising access to users and IT assets include: business role; physical location; remote access; time; patch and anti-malware status; software; operating system; device; and method of connectivity.
39. The provision of access involves the following process stages:
  - (a) identification and authentication: determination of who or what is requesting access and confirmation of the purported identity;
  - (b) authorisation: assessment of whether access is allowed to an IT asset by the requestor based on the needs of the business and the level of IT security (trust) required.

Identification, authentication and access authorisation processes are applicable to both users and IT assets.

## Identification and authentication techniques

40. A regulated institution would normally take appropriate measures to identify and authenticate users or IT assets. The required strength of authentication would normally be commensurate with risk.
41. Common techniques for increasing the strength of identification and authentication include the use of strong password techniques (i.e. increased length, complexity, re-use limitations and frequency of change) and increasing the number and/or type of authentication factors used. Authentication factors include something a person knows<sup>20</sup>, has<sup>21</sup> and is<sup>22</sup>.
42. The following are examples where increased authentication strength is typically required, given the risks involved:
  - (a) administration or other privileged access to sensitive or critical IT assets;
  - (b) remote access (i.e. via public networks) to sensitive or critical IT assets; and
  - (c) high-risk activities (e.g. third-party fund transfers, creation of new payees).
43. The period for which authentication is valid would be commensurate with the risk. Common techniques for achieving this include session timeouts and the use of time-limited one-time passwords.

### Access control techniques

44. A regulated institution would typically deploy the following controls to limit access to IT assets, based on a risk assessment:
  - (a) granting access based on a risk assessment. The use of contractors and temporary staffing arrangements may elevate the risk for certain roles;

<sup>20</sup> e.g. user IDs and passwords.

<sup>21</sup> e.g. a security token or other devices in the person's possession used for the generation of one-time passwords.

<sup>22</sup> e.g. retinal scans, hand scans, signature scans, digital signature, voice scans or other biometrics.

- (b) implementation of role-based access profiles which are designed to ensure effective segregation of duties;
  - (c) prohibiting the sharing of accounts and passwords (including generic accounts);
  - (d) changing of default passwords and user names;
  - (e) removal of access rights whenever there is a change in role or responsibility, and on cessation of employment. Access rights can then be granted in line with the new role or responsibility, without risk of unnecessary access remaining;
  - (f) processes to notify appropriate personnel of user additions, deletions and role changes;
  - (g) audit logging and monitoring of access to IT assets by all users;
  - (h) regular reviews of user access by IT asset owners to ensure appropriate access is maintained;
  - (i) multi-factor authentication for privileged access, remote access and other high-risk activities;
  - (j) generation, in preference to storage, of passwords/PINs<sup>23</sup> where these are used to authorise high-risk activities (e.g. debit/credit card and internet banking transactions); and
  - (k) two-person rule applied to extremely sensitive IT assets (e.g. encryption keys<sup>24</sup>, PIN generation, debit/credit card databases).
45. For accountability purposes, a regulated institution would normally ensure that users and IT assets are uniquely identified and their actions are auditable.

## **Data/information leakage**

46. 'Data leakage'<sup>25</sup> is defined as the unauthorised removal, copying, distribution, capturing or other types of disclosure of sensitive data/information. Access to data removal methods would normally be subject to risk assessment and only granted where a valid business need exists.
47. Controls, commensurate with the sensitivity and criticality of the data/information involved, would normally be implemented where sensitive data/information is at risk of leakage. Examples of such data leakage methods include the use of: portable computing devices (e.g. laptops, PDAs, mobile phones); portable storage devices (e.g. USB flash drives, portable hard drives, writable disks); electronic transfer mechanisms (e.g. email, instant messaging); and hard copy.
48. Common controls for data/information removal methods would normally be commensurate with risk. Users with a greater level of access to sensitive data/information would be subject to an increased level of scrutiny. Such controls could include:
- (a) authorisation, registration and regular review of users and associated transfer mechanisms and devices (including printers);
  - (b) appropriate encryption, cleansing and auditing of devices;
  - (c) appropriate segmentation of data/information based on sensitivity and access needs;
  - (d) appropriate blocking, filtering and monitoring of electronic transfer mechanisms and printing; and
  - (e) monitoring for unauthorised software and hardware (e.g. key loggers, password cracking software, wireless access points, business implemented technology solutions).

23 Personal Identification Numbers (PINs) are a secret (usually numeric) password shared between a user and a system that can be used to authenticate the user to the system.

24 Refer to Attachment F for further guidance.

25 Sometimes referred to as data loss.

49. In APRA's view, wholesale access to sensitive data/information<sup>26</sup> would be highly restricted to reduce the risk exposure to significant data leakage events. Industry experience of actual instances in this area includes the leakage of debit/credit card details and the sale/trade or exploitation of customer identity information.

### **Cryptographic techniques to restrict access**

50. In APRA's view, cryptographic techniques would normally be used to control access<sup>27</sup> to sensitive data/information, both in storage and in transit. The strength of the cryptographic techniques deployed would be commensurate with the sensitivity and criticality of the data/information as well as other supplementary or compensating controls. (Refer to Attachment F for further guidance.)

51. In order to minimise the risk of compromise, an end-to-end approach would normally be adopted, where encryption is applied from the point of entry to final destination.

## **IT asset life-cycle management controls**

### **IT security considered at all stages**

52. APRA envisages that a regulated institution would ensure that IT security is considered at all stages of an IT asset's life-cycle<sup>28</sup>. This could involve the use of external advisers where expertise is not available internally. Life-cycle stages typically include: planning and design; acquisition and implementation; support and maintenance; and decommissioning and disposal. Regulated institutions would usually apply project management techniques to manage material changes during these stages and to ensure that IT security requirements have been adequately addressed.

53. Planning and design controls would typically be in place to ensure that IT security is embodied in the overall IT architecture. Solutions implemented would normally comply with the IT security requirements of a regulated institution (as embodied in the IT security risk management framework), including availability considerations (refer to Attachment B for further guidance).

54. Acquisition and implementation controls would typically be in place to ensure that the IT security of the technology environment is not compromised by the introduction of new IT assets. Ongoing support and maintenance controls would typically be in place to ensure that IT assets continue to meet business objectives. Examples of controls include:

- (a) change management controls to ensure that the business objectives continue to be met following change (refer to Attachment A for further guidance);
- (b) configuration management controls to ensure that the configuration minimises vulnerabilities and is defined, assessed, registered and maintained;
- (c) deployment and environment controls to ensure that development, test and production environments are appropriately segregated and enforce segregation of duties;
- (d) patch management controls to manage the assessment and application of patches to software that address known vulnerabilities in a timely manner;
- (e) service level management: mechanisms to monitor, manage and align IT security with business objectives;
- (f) capacity and performance management controls to ensure that the current and projected requirements of the business are met; and

26 e.g. contents of customer data bases or intellectual property that can be exploited for personal gain.

27 Cryptographic techniques may also be used to verify data/information integrity.

28 Refers to the life-cycle of IT assets more broadly, not just to the software development life-cycle.

- (g) service provider (including vendor) management controls to ensure that a regulated institution's IT security requirements are met by service providers.

55. Decommissioning and destruction controls are used to ensure that IT security is not compromised as IT assets reach the end of their useful life. Examples include archiving strategies and the deletion of sensitive information prior to the disposal of IT assets.

### Physical security

56. The strength of the environmental controls would normally be commensurate with the sensitivity and criticality of the IT asset(s). The absence of physical security could compromise the effectiveness of other IT security controls. A regulated institution would normally deploy the following environmental controls:

- (a) location and housing that provide a level of protection from natural and man-made threats;
- (b) restricted access to sensitive areas. This includes procedures for handling access by staff, third party providers and visitors; and
- (c) monitoring and alert mechanisms for the detection of compromises of environmental controls including: temperature; water; smoke and access sensors/alarms; service availability alerts (power supply, telecommunication, servers); and access log reviews.

### Secure software development

57. A regulated institution would normally consider IT security at all stages of software development. This would assist in maintaining confidentiality, integrity and availability by improving software quality and minimising exposure to vulnerabilities (refer to Attachment D for further guidance).

### IT security technology solutions

58. A regulated institution typically deploys specific technology solutions in key locations to control or monitor the security of various IT assets. Examples include: firewalls; network access control; intrusion detection/prevention devices; anti-malware; encryption and monitoring/log analysis tools. The degree of reliance that is placed on these technology solutions and their criticality and sensitivity necessitate a heightened set of life-cycle controls, including but not limited to:

- (a) guidelines outlining when IT security-specific technology solutions should be used;
- (b) standards documenting the detailed objectives and requirements of individual IT security-specific technology solutions;
- (c) authorisation of individuals who can make changes to IT security-specific technology solutions. This would normally take into account segregation of duties issues; and
- (d) regular assessment of the IT security-specific technology solutions configuration, assessing both continued effectiveness as well as identification of any unauthorised changes.

### End-user developed/configured software

59. Current technologies allow for end-users to develop software for the purpose of automating day-to-day business process or facilitating decision-making. In addition, software is increasingly designed to be configurable by end-users. This creates the risk that inadequate life-cycle controls are in place for critical IT assets.
60. A regulated institution would normally introduce processes to identify the existence of end-user developed/configured software and assess its risk exposure. In APRA's view, any IT software asset that is critical to achieving the objectives of the business, or processes sensitive data/information, would comply with the relevant life-cycle management controls of the institution.

## Legacy technologies

61. IT assets that have been implemented prior to an institution's current IT security management framework may not comply with the framework's requirements. In such instances, the institution would typically, as part of its risk management processes, formulate a strategy for either the replacement of the IT assets and/or the implementation of appropriate compensating controls commensurate with the institution's risk appetite. Variations from the IT security management framework would normally be captured in an exemption register.

## Emerging technologies

62. New technologies potentially introduce a set of additional risk exposures (both known and unknown). A regulated institution would normally apply appropriate caution when considering the introduction of new technologies.
63. Typically, a regulated institution would only authorise the use in a production environment of technologies:
  - (a) that have matured to a state where there is a generally agreed set of industry-accepted controls to manage the security of the technology; or
  - (b) where compensating controls are sufficient to comply with the institution's risk appetite (e.g. network segmentation).
64. A regulated institution may find it useful to develop a technology authorisation process and maintain an approved technology register to facilitate this. The authorisation process would typically involve a risk assessment balancing the benefits of the new technology with the risk (including an allowance for uncertainty).

## Monitoring and incident management

### Monitoring processes

65. A regulated institution would normally have monitoring processes in place to identify events and unusual patterns of behaviour that could impact on the security of IT assets. The strength of the monitoring controls would typically be commensurate with the criticality and sensitivity of an IT asset. APRA envisages that alerts would be investigated in a timely manner, with an appropriate response determined.
66. Common monitoring processes include:
  - (a) activity logging including exceptions to approved activity (e.g. device, server and network activity; security sensor alerts);
  - (b) environment and customer profiling;
  - (c) checks to determine if IT security controls are operating as expected and are being complied with; and
  - (d) monitoring staff or third-party access to sensitive data/information to ensure it is for a valid business reason.
67. APRA envisages that a regulated institution would establish a clear allocation of responsibility for regular monitoring, with appropriate processes and tools in place to manage the volume of monitoring required, thereby reducing the risk of an incident going undetected.
68. Highly sensitive and/or critical IT assets would typically have logging enabled to record events and monitored at a level commensurate with the level of risk.
69. Users with elevated access entitlements (e.g. system administrators) would normally be subject to a greater level of monitoring in light of the heightened risks involved.

70. Access controls and segregation of duties would normally be used as a means to safeguard the integrity of the monitoring logs and processes.

### **Incident management**

71. APRA envisages that a regulated institution would develop appropriate processes to manage all stages of an incident that could impact on services including detection, identification, containment, investigation, evidence gathering, resolution, return to business-as-usual and reducing the risk of similar future events. Common incident types include:
- (a) outages/degradation of services due to hardware, software or capacity issues;
  - (b) unauthorised access to IT assets;
  - (c) data leakage;
  - (d) identity theft;
  - (e) malicious software and hardware;
  - (f) fraud;
  - (g) failed backup processes;
  - (h) denial of service attacks; and
  - (i) data integrity issues.
72. A regulated institution would normally have clear accountability and communication strategies to limit the impact of IT security incidents. This would typically include defined mechanisms for escalation and reporting to the Board and senior management and customer communication where appropriate (refer to Attachment E for further guidance). Incident management strategies would also typically assist in compliance with regulatory requirements. Institutions would normally notify APRA after experiencing a major incident.
73. Incidents would typically be subject to root cause analysis, where the underlying cause(s) of the incident is identified and analysed and controls adjusted to reduce the likelihood and impact of a future occurrence.

### **Accountability and audit trails**

74. APRA envisages that a regulated institution would ensure audit trails exist for IT assets that: satisfy the institution's business requirements (including regulatory and legal); facilitate independent audit; assist in dispute resolution (including non-repudiation); and assist in the provision of forensic evidence if required. This could include, as applicable:
- (a) the opening, modification or closing of customer accounts;
  - (b) any transaction with financial consequences;
  - (c) authorisations granted to customers to exceed a pre-approved limit;
  - (d) accessing or copying of sensitive data/information; and
  - (e) granting, modification or revocation of systems access rights or privileges for accessing sensitive IT assets.
75. Audit trails would typically be secured to ensure the integrity of the information captured, including the preservation of evidence. Retention of audit trails would normally be in line with business requirements (including regulatory and legal).

## **IT security reporting and metrics**

### **Regular reporting**

76. A regulated institution would typically develop a formalised IT security reporting framework that provides operational information and oversight across the various dimensions of the IT security risk management framework. The framework would incorporate clearly defined reporting and escalation thresholds and reflect the various audiences responsible for either acting on or reviewing the reports. Reporting mechanisms would typically ensure appropriate consideration of both risk and control dimensions.

77. In APRA's view, there would normally be sufficient management reporting to enable effective oversight of the performance of the IT security management function in meeting its stated objectives. Reporting may include: risk profile(s); exposure analysis; progress against strategy; incident analysis; system capacity and performance analysis; recovery status; infrastructure and software analysis; project assessment and analysis; audit findings and ageing reports; and fraud analysis.

### Effective IT security metrics

78. IT security metrics can be useful mechanisms for assessing the success of the IT security risk management framework in maintaining confidentiality, integrity and availability, and are usually included in IT security reporting. In APRA's view, each dimension of the IT security risk management framework would be measured by at least one metric to enable the monitoring of progress towards set targets and the identification of trends.
79. APRA envisages that the use of metrics would be targeted towards the areas of greatest criticality and sensitivity as determined through the risk assessment process. Effective metrics are specific, measurable, business-impact oriented, controllable and reportable. In addition, a comprehensive set of metrics would include both backward – and forward-looking measures (i.e. key performance indicators (KPIs) and key risk indicators (KRIs)).

## IT security assurance

### Assurance program

80. APRA expects that a regulated institution would seek regular assurance that IT assets are appropriately secured and that its IT security risk management framework is effective. This would normally be executed through a formal program of work that facilitates a systematic assessment of the IT security risk and control environment over time.

### Frequency of assurance

81. A regulated institution would benefit from a multi-year schedule of testing that incorporates both adequacy and compliance-type reviews, with the program of work determined on a risk basis. Additional assurance work may be triggered by changes to vulnerabilities/threats or material changes to IT assets.
82. The schedule of testing would typically ensure that all aspects of the IT security control environment are assessed over time, commensurate with the sensitivity and criticality of the IT assets. In APRA's view, annual testing (as a minimum) would be normal for IT assets exposed to 'un-trusted' environments<sup>29</sup>.

### Independence

83. Traditionally, assurance work has been executed by Internal Audit. However, given the specialist nature of this work, other appropriately trained and sufficiently independent (to avoid conflicts of interest) IT security experts could be used to complement such work. APRA envisages that any findings would be reported and monitored using the established audit/compliance issue tracking process.

<sup>29</sup> Environments where a regulated institution is unable to enforce IT security policy (e.g. public networks).

## Attachment A: Change management

1. APRA envisages that a regulated institution would implement controls to manage change to IT assets with the aim of maintaining confidentiality, integrity and availability. This includes changes to hardware, software (including associated configurations) and data fixes.
2. Key components of effective change control include: registration of proposed changes; impact assessment; change scheduling; and approval of changes prior to deployment into the production environment. Change management aims to balance the need for change with the potential detrimental impact of the change. Common components of change control that a regulated institution would normally deploy include:
  - (a) changes to the production environment (including planned and emergency changes to software, hardware and data) developed and verified in another environment<sup>30</sup>, sufficiently segregated from production so as to avoid any compromise of IT security;
  - (b) testing environments that are representative of production in order to reduce the risk of changes in behaviour when deployed to production;
  - (c) IT security review points at all stages of the change life-cycle to ensure that security controls are identified, designed, constructed and tested so that the level of security continues to meet business objectives. The level of review would typically be commensurate with the risk associated with the change and could range from peer review to independent vulnerability assessment;
  - (d) various levels of formal testing (such as unit, module, regression, system, integration, sociability, performance, security and user acceptance testing) followed by formal sign-off (from the business and other impacted areas) prior to deployment into the production environment;
  - (e) desensitising production data/information when it is used for testing purposes;
  - (f) segregation of duties in place between staff actioning a change and those deploying a change to production;
  - (g) changes scheduled and reviewed to ensure that multiple changes made at the same time do not conflict with each other;
  - (h) processes that provide reasonable assurance that system recovery procedures and components are in place at the time of deployment to production so that recovery requirements can be met; and
  - (i) implementation plans that include, as appropriate, a back-out/fall-back strategy that provides reasonable assurance that a failed deployment can be reversed or otherwise managed.

<sup>30</sup> A regulated institution would typically run multiple environments reflecting the various stages of software development and testing (e.g. development, system testing, user acceptance testing, staging, etc.).

## Attachment B: Resilience and recovery

1. Regulated institutions could incur substantial losses as a result of disruptions to critical business operations. Resilience and recovery capabilities for IT assets are an important component in ensuring that institutions are able to meet financial and service obligations.
2. Resilience refers to techniques that ensure systems remain available in the event of failure of individual components. Recovery capability ensures that the IT environment can meet business recovery objectives<sup>31</sup> in the event that IT assets have become unavailable. In general, resilience reduces the likelihood of IT assets becoming unavailable, whereas recovery reduces the impact of an incident that has compromised availability.
3. APRA envisages that, for critical IT assets, a regulated institution would implement appropriate resilience capabilities and recovery strategies to cater for scenarios threatening an asset's availability. The level of resilience and recovery capability required by an institution would be based on an assessment of the IT assets' criticality. This is normally assessed through a business impact analysis. One of the outcomes of this process would typically be the establishment of formal IT asset recovery objectives and associated arrangements. Refer to APRA's Prudential Standards and Practice Guides on Business Continuity Management for APRA's requirements and guidance in this area.<sup>32</sup>
4. Regardless of the level of resilience, APRA envisages that a regulated institution would still develop formal recovery plans to enable recovery of critical IT assets to a known state, sufficient to enable restoration of critical business operations in line with business needs.
5. A critical facet with respect to recovery is the usage of additional data processing sites. APRA envisages that a regulated institution would have formal arrangements in place to allow for recovery to an alternate processing site in the event of a disaster impacting the primary site(s).
6. There is a trend for regulated institutions to implement a highly resilient data centre model where production processing is distributed across multiple data centres. In APRA's view, regulated institutions would still maintain recovery capability to address the risk of a logical compromise to the IT security in one data centre (e.g. failed change, malware, data corruption, etc.) replicating to other data centres.
7. Recovery plans refer to documented procedures and information including:
  - (a) plans for responding to a material disruption to services;
  - (b) resources and associated timeframes required in order to recover services;
  - (c) relevant information pertaining to alternate sites for the recovery of business and/or IT operations and details of the location and procedures for gaining access to off-site data storage;
  - (d) procedures for the recovery and restoration of critical services in an orderly manner to the recovery point, within the required timeframe, and to a level of service agreed with the business;
  - (e) procedures to verify the recovery state and integrity of IT assets;

<sup>31</sup> This includes recovery timeframes (recovery time objective), point in time to which IT assets have been recovered to (recovery point objective), and processing capacity.

<sup>32</sup> *Prudential Standard APS 232 Business Continuity Management (APS 232); Guidance Note AGN 232.1 Risk Assessment and Business Continuity Management (AGN 232.1); Prudential Standard GPS 222 Business Continuity Management (GPS 222); Guidance Note GGN 222.1 Risk Assessment and Business Continuity Management (GGN 222.1); Prudential Standard LPS 232 Business Continuity Management (LPS 232); Prudential Practice Guide LPG 232 Business Continuity Management (LPG 232); and Prudential Practice Guide PPG 233 Pandemic Planning and Risk Management (PPG 233).*

- (f) a communication plan for notifying key internal and external stakeholders if a regulated institution's recovery plan is invoked; and
  - (g) an IT business continuity plan. This documentation would typically be focused on operational processes and procedures the IT unit would follow while operating from an alternate site.
8. Where the enactment of a recovery plan is reliant upon a third party, appropriate arrangements would normally be established to secure services within the timeframes required. It would be beneficial to verify this periodically to ensure recovery timeframes are achievable.
  9. A regulated institution would normally test system resilience and recovery capabilities at least annually to verify that business continuity and recovery requirements are achievable and that recovery plans remain current. The institution would benefit from a multi-year schedule of testing that incorporates verification of recovery at both the whole-of-site and component levels.
  10. It is important that the success criteria for the testing of resilience and recovery are clearly defined, including the circumstances under which re-testing would be required. Test results and associated follow-up actions are typically formally tracked and reported.
  11. It is also important that controls are in place to ensure that IT security is not compromised throughout the testing process. This would include access to and the secure destruction of sensitive data/information after the test.
  12. APRA envisages that a regulated institution would regularly backup critical and sensitive IT assets, regardless of the level of resilience in place. Appropriate controls would be implemented to ensure the security of the backups is maintained while in transit and storage, typically via physical security and cryptographic techniques. Recovery procedures would normally be regularly tested to ensure that they are adequate to achieve effective recovery from backups.
  13. All components required to enact the recovery plans would typically be located at a sufficient distance from the operational site(s) so that they are not impacted by the same disaster. This includes: recovery sites and hardware; backups of data/information and software; and copies of the recovery plans.
  14. In the case where a regulated institution has contractual arrangements for recovery facilities that are shared with a number of other organisations, the contract between a regulated institution and the alternate site provider would normally guarantee access to the minimum IT assets required to operate under a disaster scenario.
  15. Refer to APRA's Prudential Standards, Practice Guides and guidance notes with respect to Business Continuity Management and Outsourcing for APRA's requirements and guidance in this area.<sup>33</sup>

### **Offshore IT assets**

16. For regulated institutions that have critical system components (processing and/or data) located offshore, sound practice would involve the development of recovery strategies, plans and associated arrangements, to address the scenario where the component located offshore becomes unavailable for an undefined period of time. This would address scenarios based on man-made and natural disaster events, and the financial failure of the institution maintaining the systems.

<sup>33</sup> APS 232; AGN 232.1; GPS 222; GGN 222.1; LPS 232; LPG 232; PPG 233; *Prudential Standard APS 231 Outsourcing* (APS 231); *Prudential Standard GPS 231 Outsourcing* (GPS 231); *Prudential Standard LPS 231 Outsourcing* (LPS 231); *Prudential Practice Guide PPG 231 Outsourcing* (PPG 231) and *Superannuation guidance note SGN 130.1 Outsourcing* (SGN 130.1).

17. In APRA's view, recovery strategies, plans and associated arrangements would be designed to ensure that a regulated institution maintains control over the IT assets pertaining to the Australian-regulated operations. This would be facilitated by:
  - (a) documentation that clearly identifies the relevant IT assets (e.g. an asset inventory and systems architecture diagrams);
  - (b) sufficient segregation of IT assets pertaining to the Australian-regulated operations from other systems to allow their separation if required; and
  - (c) contractual protection to ensure access to IT assets pertaining to the Australian-regulated operations. This includes defining ownership and jurisdiction of the IT assets.
18. APRA envisages that recovery of IT assets pertaining to the Australian-regulated operations would be to a location that is not likely to be subject to the same disaster (including man-made).
19. In the case of a foreign subsidiary, under the scenario of the financial failure of the Group, recovery plans would normally be in place to enable repatriation of sufficient data/information to enable an orderly transition of operations (e.g. customer balances and transaction history).

## Attachment C: Service provider management

1. IT security risks need to be appropriately managed regardless of whether activities and associated IT assets are under the direct control of a regulated institution or have been outsourced to a service provider. Where a service provider (including a software vendor) has been engaged, the due diligence, the formulation of the service agreement and the ongoing monitoring of the service provider would all normally be structured so as to facilitate oversight of the management of all such risks, commensurate with the sensitivity and criticality of the IT assets impacted.
2. Appropriate due diligence would normally ensure an assessment as to the robustness of the IT security risk management framework of the service provider, and alignment with a regulated institution's own framework.
3. Effective service agreements normally embody a regulated institution's IT security principles and associated requirements. A regulated institution would normally reflect relevant areas of its IT security framework in the agreement, thereby ensuring that its IT security stance is not compromised or weakened by the use of a service provider.
4. The service agreement would include reporting mechanisms that ensure adequate oversight of IT security risk management by the service provider. Oversight would typically involve the assessment of the following items against a regulated institution's IT security requirements:
  - (a) service level reporting against agreed IT security metrics (e.g. availability, incident response timeframes);
  - (b) results of business continuity and recovery testing and associated follow-up actions;
  - (c) post-incident reporting including rectification actions, timeframes and root cause analysis;
  - (d) relevant compliance, audit and IT security testing reports and associated follow-up actions;
  - (e) handling of sensitive data/information; and
  - (f) notification of material changes by the service provider to the technology environment; relevant policies, standards, and procedures; or changes to personnel, including the use of subcontractors.
5. Refer to APRA's Prudential Standards and guidance on Outsourcing for APRA's requirements and guidance in this area.<sup>34</sup>

<sup>34</sup> APS 231; GPS 231; LPS 231; PPG 231 and SGN 130.1.

## Attachment D: Secure software development

1. A regulated institution would normally implement secure software development techniques for software assets, with a focus typically on the more sensitive or critical software assets. This will assist in maintaining confidentiality, integrity and availability by improving the general quality and vulnerability profile of the software, thereby ensuring that it:
  - (a) continues to function as intended regardless of unforeseen circumstances; and
  - (b) has a reduced propensity to be misused either intentionally (e.g. fraud) or inadvertently.
2. APRA envisages that a regulated institution would include IT security considerations throughout the software development life-cycle including requirements-gathering, design, programming, testing and implementation phases. Ongoing security of existing software would also normally be considered as part of change management and as new vulnerabilities are identified. Typical factors to consider for the development of secure software include:
  - (a) requirements and design. IT security requirements are best explicitly identified as part of the design, requirements definition and technical specification of the software. Considerations when designing secure software can include: software modularisation; where on the network the software is located; what privileges the software executes under; and to what IT security standards and guidelines the software specifications are written.
    - (b) standards and guidelines. In APRA's view, the body of knowledge for developing secure software would normally be embodied in a set of standards and guidelines. Typically, standards will exist for each programming language, taking into account known vulnerabilities and good IT security practices. It is important that standards remain aligned with industry developments (such as emerging vulnerabilities/threats and associated compensating controls). In developing software standards and guidelines, consideration would typically be given to:
      - (i) common software requirements such as authentication, authorisation, session management, data validation, cryptography, logging, configuration, auditing, deployment and maintenance;
      - (ii) techniques for addressing common weaknesses such as poor exception and error handling; weak file and group permissions; use and storage of temporary files; unnecessary code; insecure system calls; poor password handling; and susceptibility to buffer overflow, code insertion and resource (e.g. memory) leakage;
      - (iii) software defence techniques against known vulnerabilities; and
      - (iv) approaches for secure input/output handling.

- (c) security reviews. Software reviews, tools and testing are normally used to identify vulnerabilities prior to implementation. Several assessments throughout the software life-cycle may also be appropriate. The level and type of review would normally be commensurate with the level of risk, sensitivity and criticality of the software. Common types of reviews and testing include vulnerability assessments (internal and external) and code reviews that would typically assess:
  - (i) whether IT security requirements have been met;
  - (ii) whether the software works as intended; and
  - (iii) expected behaviour when erroneous input is supplied.
- 3. A regulated institution would typically implement source code review (both peer reviews, as well as automated analysis reviews) as part of the software testing strategy to identify insecure code. Source code reviews are normally conducted by an individual other than the original author. The individual would normally be functionally independent, appropriately trained and have the necessary competence.
- 4. A regulated institution may find it useful to maintain a register of approved software development tools and associated usage. The institution would normally enforce compliance with the register for the purposes of quality control, avoiding compromises of the production environment and reducing the risk of introducing unexpected vulnerabilities. This would not preclude the use of other tools in a non-production environment for the purposes of evaluation and experimentation.
- 5. A regulated institution would normally implement roles, responsibilities and tools for managing the registration and deployment of source code to ensure that IT security requirements are not compromised.

## Attachment E: Customer protection

1. APRA envisages that a regulated institution would revise and regularly review customer IT security advice to ensure that it remains adequate and appropriate relative to the institution's risk profile. To help reduce the risk of being targeted for the perpetration of fraud, a regulated institution may find it beneficial to compare customer advice with its peers, and the industry more broadly, on a regular basis.
2. A regulated institution would normally advise on measures for customers to protect themselves against fraud and identity theft. Examples of advice given would typically include:
  - (a) not disclosing personal, financial or debit/credit card information unnecessarily or where the integrity of the recipient is suspect;
  - (b) when conducting banking activities, taking safeguards to ensure no one else is able to observe or access credentials or other IT security information;
  - (c) using strong password controls by adopting passwords/PINS that are difficult to guess; changing passwords/PINS regularly; avoiding reuse of passwords/PINS; and not selecting the option on browsers for storing or retaining user identifier and password/PIN;
  - (d) remaining alert for features to verify that a website or other media is bona fide and not accepting links or redirections from other websites or media for the purpose of logging onto the institution's website;
  - (e) remaining alert for suspicious websites, emails, phone calls and other correspondence purporting to be from the institution, and reporting these immediately to the institution;
  - (f) advice as to monitoring account transactions and balances on a regular basis;
  - (g) advice as to the process to follow should a customer suspect they have been the victim of fraud/identity theft (including attempts thereof);
  - (h) reminding customers that the institution will not make unsolicited requests for sensitive customer information used for the purposes of authentication, such as passwords/PINS; and
  - (i) applying appropriate controls for securing computers and other devices used to access banking services.
3. A regulated institution's controls for reducing the risk exposure of fraudulent activity, data leakage, or identity theft (in addition to those outlined elsewhere in this PPG) would typically include:
  - (a) procedures for only collecting personal information relevant to the business activities undertaken and in compliance with relevant privacy legislation;
  - (b) procedures for ensuring that under no circumstances would a customer be asked to reveal sensitive customer information used for the purposes of authentication, such as passwords/PINS;
  - (c) publication of customer privacy and relevant IT security policies such as customer dispute handling, reporting and resolution procedures and the expected timing of the institution's response;
  - (d) usage of a second channel notification/confirmation of events (e.g. account transfers, new payees, change of address);
  - (e) implementation of appropriate limits on financial transactions; and
  - (f) documented and communicated procedures for incident monitoring and management of fraud, data leakage and identity theft.
4. When communicating with customers in relation to IT security precautions and policies, it would be more effective if regulated institutions used plain language. In addition, it is normally preferable to use consistent information across all communication channels (e.g. websites, account statements, promotional material and direct customer contact).

## Attachment F: Cryptographic techniques

1. Cryptographic techniques refer to methods used to encrypt<sup>35</sup> data/information, confirm its authenticity or verify its integrity. The following are examples where regulated institutions could deploy cryptographic techniques given the risks involved :
  - (a) transmission and storage of critical and/or sensitive data/information in an 'un-trusted' environment or where a higher degree of security is required;
  - (b) detection of any unauthorised alteration of data/information;
  - (c) verification of the authenticity of transactions or data/information; and
  - (d) the generation of customer PINs which are typically used for debit/credit cards and online services.
2. There are a variety of cryptographic techniques that a regulated institution can apply, each effective for a specific purpose. Cryptographic techniques can also be deployed that have varying degrees of strength (i.e. levels of sophistication of ciphers (algorithm) or hash<sup>36</sup> functions and the length of cryptographic keys<sup>37</sup> applied).
3. A regulated institution would normally select appropriate cryptographic techniques based on the control effectiveness required and the sensitivity and criticality of the data/information involved. The institution's chosen cryptographic techniques would normally be reviewed on a regular basis to ensure that they remain commensurate with the risk environment.
4. APRA envisages that a regulated institution would select algorithms from the population of well established and proven international standards that have been subjected to rigorous public scrutiny and verification of effectiveness (e.g. Triple DES<sup>38</sup>, AES<sup>39</sup> etc.). The length of a cryptographic key would typically be selected to render a brute force attack<sup>40</sup> impractical (i.e. would require an extremely long period of time to breach using current computing capabilities).
5. Cryptographic key management refers to the generation, distribution, storage, renewal, revocation, recovery, archiving and destruction of encryption keys. Effective cryptographic key management ensures that controls are in place to reduce the risk of compromise of their security. Any compromise to the security of cryptographic keys may lead to a compromise of the security of the IT assets protected by the cryptography technique deployed.
6. A regulated institution would typically deploy, where relevant, the following controls to limit access to cryptographic keys, based on a risk assessment:
  - (a) additional physical protection of equipment used to generate, store and archive cryptographic keys;
  - (b) use of cryptographic techniques to maintain cryptographic key confidentiality;
  - (c) segregation of duties, with no single individual having knowledge of the entire cryptographic key (i.e. two-person controls) or having access to all the components making up these keys;

35 Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Decryption is the reverse process.

36 A hash function takes data and returns a fixed-size bit string called the hash value. Any change to the data will change the hash value.

37 A piece of auxiliary information which changes the detailed operation of the cipher.

38 Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA) block cipher.

39 Advanced Encryption Standard (AES) block cipher.

40 A brute force attack is a method of defeating a cryptographic scheme by systematically trying a large number of possibilities.

- (d) predefined activation and deactivation dates for cryptographic keys, limiting the period of time they remain valid for use. The period of time a cryptographic key remains valid commensurate with the risk;
  - (e) clearly defined cryptographic key revocation processes; and
  - (f) the deployment of detection techniques to identify any instances of cryptographic key substitution.
7. A regulated institution would typically utilise tamper resistant devices to store and generate cryptographic keys, generate PINs and perform encryption and decryption. In most cases this would involve the use of Hardware Security Modules<sup>41</sup> (HSMs) or similarly secured devices. These devices would be appropriately secured both physically and logically.

<sup>41</sup> Hardware Security Module is a type of secure crypto-processor that provides for the secure generation and storage of cryptographic and other sensitive data/information.



Telephone  
1300 13 10 60

Email  
[contactapra@apra.gov.au](mailto:contactapra@apra.gov.au)

Website  
[www.apra.gov.au](http://www.apra.gov.au)

Mail  
GPO Box 9836  
in all capital cities  
(except Hobart and Darwin)