PRUDENTIAL PRACTICE GUIDE

Draft CPG 234 Information Security

March 2019

Disclaimer and Copyright

Contents

About this guide

Prudential practice guides (PPGs) provide guidance on APRA's view of sound practice in particular areas. PPGs frequently discuss statutory requirements from legislation, regulations or APRA's prudential standards, but do not themselves create enforceable requirements. PPGs target areas where APRA continues to identify weaknesses as part of its ongoing supervisory activities, and do not seek to provide an all-encompassing framework, or to replace or endorse existing industry standards and guidelines.

This PPG aims to assist regulated entities in maintaining information security. It is designed to provide guidance to Boards, senior management, risk management and information security specialists (management and operational).

Subject to meeting APRA's prudential requirements, regulated entities have the flexibility to maintain information security in a manner best suited to achieving their business objectives. Not all of the practices outlined in this PPG will be relevant for every regulated entity and some aspects may vary depending upon the size and nature of the entity.

Introduction

1. Cyber-attacks are increasing in frequency, sophistication and impact, with perpetrators continually refining their efforts to compromise systems, networks and information world-wide. The financial sector is one of the more prominent targets for such attacks. A key driver of this trend is the increasing usage of technology by the financial sector to improve customer service and operational efficiency. Consequently, stakeholders including Boards of directors (Boards), senior management, shareholders, customers and regulators have heightened expectations for the effective safeguarding of information assets underpinned by an organisational culture that promotes information security.

2. This PPG targets areas where weaknesses in information security management continue to be identified as part of APRA's ongoing supervision activities. It is also intended to provide guidance with respect to the implementation of *Prudential Standard CPS 234 Information Security* (CPS 234). The intended outcome is to ensure that APRA-regulated entities take measures to be resilient against information security incidents, including cyber-attacks, so that under all reasonable circumstances financial promises made by APRA-regulated entities to beneficiaries are met.

3. This PPG aims to provide guidance to Boards, senior management, risk management and information security specialists (both management and operational) of APRA-regulated entities. The multiple audiences reflect the pervasive nature of information security threats and vulnerabilities and the need for sound practices and a solid business understanding in order to maintain an information security capability commensurate with those threats and vulnerabilities. It also reflects that APRA-regulated entities have developed distinct practices and disciplines to manage information security risk, information technology (IT) risk and operational risk. In APRA's view, these are all necessary and complementary disciplines.

4. While this PPG provides guidance for safeguarding information assets it does not seek to be all-encompassing. APRA expects that regulated entities will implement appropriate information security controls informed by contemporary sound industry practices, including in areas not explicitly addressed by this PPG. Additionally, this PPG is not intended to replace or endorse existing industry standards and guidelines. A regulated entity would typically use discretion in adopting industry standards and guidance it considers fit-for-purpose in specific control areas.

5. Subject to APRA's prudential standards, an APRA-regulated entity has flexibility to maintain its information security capability in the way most suited to achieving its information security objectives. Where the content of this PPG refers to matters contained in prudential standards and PPGs other than CPS 234, the intent is to provide guidance on matters that directly relate to information security.

6. In a number of areas, this PPG provides examples of practices to illustrate a range of controls that could be deployed to address a stated principle. These examples are not

intended to be exhaustive compliance checklists. Additionally, attachments have been included in areas where APRA has determined that more detailed guidance is warranted.

Considerations for the Board

7. This section sets out key information a Board could consider in relation to its responsibilities under CPS 234. The remainder of the PPG elaborates on this information, and contains additional detail on information security aimed at a broader audience. A Board member may find it beneficial to acquaint themselves with this additional detail as necessary.

8. Under CPS 234, the Board of an APRA-regulated entity is ultimately responsible for the information security of the entity. In order for a Board to be able to more effectively discharge its responsibilities (including oversight, seeking assurance and, as appropriate, challenging management), it could consider the following:

    a) roles and responsibilities — clearly outline for management how the Board expects to be engaged, including delegation of responsibilities, escalation of risks, issues and reporting requirements (including schedule, format, scope and content). Refer to Attachment H for common examples of the types of information that the Board might find useful to effectively fulfil its role and discharge its responsibilities;

    b) information security capability — consider the sufficiency of the regulated entity's information security capability in relation to vulnerabilities and threats; ensure sufficiency of investment to support the information security capability; and review progress with respect to execution of the information security strategy;

    c) policy framework — whether information security policies reflect Board expectations;

    d) implementation of controls — regularly seek assurance from and, as appropriate, challenge management on reporting regarding the effectiveness of the information security control environment and the overall health of the entity's information assets;

    e) testing control effectiveness — regularly seek assurance from and, as appropriate, challenge management on the sufficiency of testing coverage across the control environment; form a view as to the effectiveness of the information security controls based on the results of the testing conducted; and

    f) internal audit — consider the sufficiency of internal audit's coverage, skills, capacity and capabilities with respect to the provision of independent assurance that information security is maintained; form a view as to the effectiveness of information security controls based on audit conclusions; and consider where further assurance, including through expert opinion or other means, is warranted.

9. In considering the above, the Board would normally take into account the use of third parties and related parties (including group functions) by the APRA-regulated entity.

Roles and responsibilities

Board delegations

10. APRA does not seek to impose restrictions on a Board's ability to delegate information security roles and responsibilities to Board sub-committees, management committees or individuals. However, APRA expects that a Board would clearly outline how it expects to be engaged with respect to information security, including escalation of risks, issues and reporting. Refer to Attachment H for common examples of the types of information that the Board might find useful in this regard.

Clearly defined roles and responsibilities

11. Definition of information security-related roles and responsibilities is typically achieved through a combination of role statements, policy statements, reporting lines and charters of governing bodies. Common governing bodies and individuals with decision-making, approval, oversight, operations and other information security roles and responsibilities typically include:

    a) information security steering/oversight committee;

    b) risk management committee (Board and management levels);

    c) Board audit committee;

    d) executive management/executive management committee;

    e) chief information officer (CIO)/IT manager;

    f) chief information security officer (CISO)/IT security manager;

    g) information security operations/administration; and

    h) management (business and IT).

12. Information security roles and responsibilities are typically located in separate business areas, as well as within the IT function itself and in third parties and related parties. This can result in issues such as a lack of ownership, unclear accountabilities, ineffective oversight and fragmentation of practices with respect to information security. APRA-regulated entities could address these issues by maintaining clear delineation between the responsibilities of each area and implementing compensating measures. Compensating measures could include establishing a *virtual* security group comprised of individuals with information security roles and responsibilities.

Sufficient and timely information

13. The Board, governing bodies and individuals would typically define their information requirements (e.g. schedule, format, scope and content) to ensure they are provided with sufficient and timely information to effectively discharge their information security roles and responsibilities. Reporting to governing bodies would normally be supported by defined escalation paths and thresholds. An APRA-regulated entity could benefit from implementing processes for periodic review of audience relevance and fitness for use.

14. In APRA's view, effective information security reporting normally incorporates both quantitative and qualitative content. For non-technical audiences, technical information and metrics would be supplemented with appropriate thematic analysis and commentary on business implications. Attachment H illustrates various information security reporting and metrics that governing bodies and individuals could find useful regarding information security.

Information security capability

Assessing sufficiency of capability

15. In discharging its responsibility for information security, an APRA-regulated entity would typically assess the sufficiency of its information security capability. This could include reviewing the adequacy of resourcing, including funding and staffing, timely access to necessary skill sets and the comprehensiveness of the control environment — preventative, detective and responsive.

16. The current threat landscape has necessitated information security capabilities that extend beyond information technology general controls to more specialised information security capabilities. These typically include:

    a) vulnerability and threat management, including situational awareness and intelligence;

    b) information security operations and administration;

    c) secure design, architecture and consultation;

    d) security testing, including penetration testing;

    e) information security reporting and analytics;

    f) incident detection and response, including recovery, notification and communication;

    g) information security investigation, including preservation of evidence and forensic analysis; and

    h) information security assurance.

Capability of third parties and related parties

17. APRA-regulated entities often place reliance on information security capabilities of third parties and related parties to provide a targeted information security capability, or as part of a wider service-provision arrangement. Accordingly, entities would have a view as to the sufficiency of resources, skills and controls of third parties and related parties. This includes consideration of sub-contracting and on-sourcing arrangements. This could be achieved through a combination of interview, service reporting, control testing, certifications, attestations, referrals and independent assurance assessments. Any capability gaps identified would be addressed in a timely manner. An APRA-regulated entity could also consider the scope, depth and independence of certifications, attestations and assurance provided and take steps to address any limitations identified.

Adaptive and forward-looking investment

18. Under CPS 234, an APRA-regulated entity must actively maintain an information security capability with respect to changes in vulnerabilities and threats. Accordingly, an entity would typically adopt an adaptive and forward-looking approach to maintaining its information security capability, including ongoing investment in resources, skills and controls. This would commonly be achieved through the execution of an information security strategy which responds to the changing environment throughout the year. The strategy could be informed by existing and emerging information security vulnerabilities and threats, contemporary industry practices, information security incidents, both internal and external, and known information security issues. Oversight of execution of the strategy is normally the responsibility of the Board or a delegated governing body with representation from across the organisation.

Policy framework

A policy hierarchy informed by a set of key principles

19. An APRA-regulated entity's information security policy framework is commonly structured as a hierarchy, with higher level policies supported by underlying standards, guidelines and procedures. A policy framework would normally be informed by a set of information security principles that guide decision-making with regard to information security (refer to Attachment A for common information security principles). Common areas addressed by a policy framework include:

    a) identification, authorisation and granting of access to information assets (refer to Attachment C for further guidance);

    b) life-cycle[1] management that addresses the various stages of an information asset's life to ensure that information security requirements are considered at each stage, from planning and acquisition through to decommissioning and destruction;

    c) management of information security technology solutions that include firewall, anti-malicious software, intrusion detection/prevention, cryptographic systems and monitoring/log analysis tools;

    d) definition of an overarching information security architecture that outlines the approach for designing the IT environment (encompassing all information assets) from a security perspective (e.g. network zones/segments, end point controls, gateway design, authentication, identity management, interface controls, software engineering and location of information security technology solutions and controls)

    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) expectations with respect to the maintenance of information security when using third parties and related parties;

    g) acceptable usage of information assets that define the information security responsibilities of end-users including staff, third parties, related parties and customers (refer to Attachment B and Attachment F for further guidance);

    h) recruitment and vetting of staff and contractors;

    i) information security roles and responsibilities;

[1] Refers to the life-cycle of information assets more broadly, not just to the software development life-cycle. The life-cycle phases consist of: planning, design, acquisition, implementation, decommissioning and disposal.

j) physical and environmental controls; and

k) mechanisms to assess compliance with, and the ongoing effectiveness of, the information security policy framework.

20. An APRA-regulated entity's information security policy framework would typically be consistent with other entity frameworks such as risk management, service provider management and project management.

Exemption handling

21. An APRA-regulated entity could consider implementing processes that ensure compliance with its information security policy framework and regulatory requirements. This could include an exemption policy defining registration, authorisation and duration requirements. Exemptions are typically administered using a register detailing nature, rationale and expiry date. APRA envisages that an entity would review and assess the adequacy of compensating controls both initially and on an ongoing basis.

22. Information assets that existed prior to an APRA-regulated entity's current information security policy framework might not comply with the current framework's requirements. In such instances, the regulated entity would typically raise an exemption and formulate a strategy for either replacing affected information assets or implementing appropriate compensating controls.

Ongoing effectiveness and completeness

23. An APRA-regulated entity would typically periodically evaluate the effectiveness and completeness of its information security policy framework through a review of incidents that have occurred as well as comparisons to peers and established control frameworks and standards. Adjustments would be made to the policy framework to ensure its continued effectiveness. This assessment would typically also be conducted in response to a material change to information assets or the business environment.

Information asset identification and classification

Classification of all information assets by criticality and sensitivity

24. A thorough understanding of an APRA-regulated entity's information assets and the impact of a security compromise of those assets is important to maintain effective information security.

25. Under CPS 234, all information assets must be classified by criticality[2] and sensitivity[3]. This includes infrastructure, ancillary systems such as environmental control systems and physical access control systems as well as information assets managed by third parties and related parties. Furthermore, APRA-regulated entities could benefit from considering the interrelationships between information assets, including identifying information assets which are not intrinsically critical or sensitive but could be used to compromise information assets which are critical or sensitive.

Classification methodology

26. In order to identify and classify information assets, an APRA-regulated entity would benefit from maintaining a classification methodology that provides clarity as to what constitutes an information asset, granularity considerations and the method for rating criticality and sensitivity. The rating could take into account the impact of an information security compromise on an information asset. Notably, an information asset could be assessed as having a different rating from the perspective of its criticality and sensitivity.

27. APRA-regulated entities record information assets in various ways, sometimes at a very granular level and sometimes at an aggregated level. For example, a system can be seen as an aggregation of the underlying components (such as applications, databases, operating systems, middleware and data sets) and treated as a single information asset for classification purposes. Alternatively, a regulated entity could choose to treat each of the underlying components as individual information assets in their own right. Ultimately, the level of granularity would be sufficient to determine the nature and strength of controls required to protect the information asset.

28. In APRA's view, where a regulated entity has chosen to aggregate a number of underlying components into a single information asset, the criticality and sensitivity

---

[2] *Criticality* is defined in paragraph 12 of CPS 234.

[3] *Sensitivity* is defined in paragraph 12 of CPS 234.

ratings for that asset would typically inherit the criticality and sensitivity ratings of the constituent components with the highest ratings.

29. In order to facilitate information asset registration and mapping of interrelationships to other information assets, APRA-regulated entities typically use an information asset inventory repository such as a configuration management database (CMDB[4]).

30. It is common for APRA-regulated entities to leverage existing business continuity impact analyses to assess an information asset's criticality. APRA-regulated entities would also typically maintain processes to systematically assess information asset sensitivity.

[4] A CMDB is a repository that holds data relating to the information assets of an organisation, including how the information assets relate to each other.

Implementation of controls

Information security controls implemented at all stages

31. Under CPS 234, an APRA-regulated entity must have information security controls to protect its information assets commensurate with, amongst other things, the stage at which the information assets are within their life-cycle. This includes ensuring that information security controls remain effective at each stage of the life-cycle of the information asset and that there is formal allocation of responsibility and accountability for the information security of an information asset to an information asset owner. Typically, the information asset owner would be an individual located within the business function which is most dependent on the information asset.

32. As the first phases of an information asset life-cycle, planning and design controls would typically be in place to ensure that information security is incorporated within the information assets of the APRA-regulated entity, the solutions implemented would typically comply with the information security requirements of an APRA-regulated entity as embodied in its information security policy framework.

33. Acquisition and implementation controls would typically be in place to ensure that information security is not compromised by the introduction of new information assets. Ongoing support and maintenance controls would typically be in place to ensure that information assets continue to meet the information security requirements of the APRA-regulated entity. Typical examples of categories of control include:

    a) change management —information security is addressed as part of the change management process and the information asset inventory is updated;

    b) configuration management —the configuration of information assets minimises vulnerabilities and is defined, assessed, registered, maintained, including when new vulnerabilities and threats are discovered, and applied consistently;

    c) deployment and environment management —development, test and production environments are appropriately segregated and enforce segregation of duties;

    d) access management controls —only authorised users, software and hardware are able to access information assets (refer to Attachment B for further guidance);

    e) hardware and software asset controls —appropriate authorisation to prevent security compromises from unauthorised hardware and software assets;

    f) network design — to ensure authorised network traffic flows and to reduce the impact of security compromises;

    g) vulnerability management controls — which identify and address information security vulnerabilities in a timely manner;

h) patch management controls — to manage the assessment and application of patches and other updates that address known vulnerabilities in a timely manner;

i) service level management mechanisms — to monitor, manage and align information security with business objectives;

j) monitoring controls — for timely detection of compromises to information security;

k) response controls — to manage information security incidents and feedback mechanisms to address control deficiencies;

l) capacity and performance management controls — to ensure that availability is not compromised by current or projected business volumes; and

m) service provider management controls — to ensure that a regulated entity's information security requirements are met.

34. Decommissioning and destruction controls are typically used to ensure that information security is not compromised as information assets reach the end of their useful life. Examples include archiving strategies and the secure data deletion (that is, deleting data using techniques to ensure data is irrecoverable) of sensitive information prior to the disposal of information assets.

35. An APRA-regulated entity could find it useful to regularly assess the completeness of its information security controls by comparison to peers and contemporary industry practices.

Vulnerabilities and threats are identified, assessed and remediated

36. An APRA-regulated entity would typically ensure that existing and emerging information security vulnerabilities and threats pertaining to critical and sensitive information assets are identified, assessed and remediated in a timely manner. This includes information assets which are not critical or sensitive but could expose those information assets that are critical or sensitive. Accordingly, an APRA-regulated entity could:

a) implement mechanisms that access and analyse timely threat intelligence regarding vulnerabilities, threats, methods of attack and countermeasures;

b) engage with stakeholders (including Government, industry participants and customers) regarding threats and countermeasures, as appropriate;

c) develop tactical and strategic remediation activities for the control environment (prevention, detection and response) commensurate with the threat; and

d) implement mechanisms to disrupt the transitions between the phases of an attack. Under the 'cyber kill chain'[5] the phases can include reconnaissance, weaponisation, delivery, exploitation, installation, command and control and actions on objectives.

End-of-life and out-of-support issues

37. An important aspect of information asset life-cycle management involves minimising vulnerabilities and maintaining supportability. Information security exposures could arise from hardware and software which is outdated or has limited or no support (whether through a third party, a related party or in-house). Technology that is end-of-life[6], out-of-support or in extended support is typically less secure by design, has a dated security model and can take longer, or is unable, to be updated to address new threats.

38. Maintaining information assets therefore necessitates a disciplined approach to information asset life-cycle management, including a comprehensive understanding of assets that support the business, as well as the potential impacts of an information security compromise of these assets. Maintenance of information assets can be facilitated through the monitoring of end-of-support dates, where available, and the active identification of systems, including those that are internally-developed and which are no longer invested in or are not secure by design. A technology refresh plan with committed resourcing can also facilitate the timely replacement of hardware and software.

39. Where extended support arrangements are in place, it is important that there is a clear understanding of the nature and effectiveness of these arrangements. Additionally, while extended or custom support arrangements may partially mitigate risk, they are often costly, could provide a false sense of security and can further delay remediation of ageing technology. Furthermore, support agreements of this nature typically provide hot-fixes or patches for critical vulnerabilities only, and remain constrained by the dated security model and design limitations of the technology.

40. To minimise information security vulnerabilities, an APRA-regulated entity would typically decommission systems:

    a) that cannot be adequately updated as new security vulnerabilities or threats are identified; and

    b) where the use of mitigating controls — such as segregation from other information assets — is not an option.

Minimise exposure to plausible worst case scenarios

41. APRA-regulated entities could consider low likelihood scenarios, which could result in an extreme impact to the regulated entity (i.e. plausible worst case). Extreme impacts can be financial or non-financial (e.g. reputational or regulatory), potentially threatening

[5] A term used by industry to describe a method for modelling intrusions on a computer network.

[6] Active investment is no longer occurring with the technology.

the ongoing ability of the APRA-regulated entity to meet its obligations. Examples of plausible worst-case scenarios include, but are not limited to:

a) malicious acts by an insider with highly-privileged access, potentially involving collusion with internal or external parties;

b) deletion or corruption of both production and backup data, either through malicious intent, user error or system malfunction; and

c) loss of, or unauthorised access to, encryption keys safeguarding extremely critical or sensitive information assets.

42. An understanding of plausible worst case scenarios can help regulated entities identify and implement additional controls to prevent or reduce the impact of such scenarios. One example is malware that infects computers and encrypts data, both on the infected computer and any connected storage, including (corporate) networks and cloud storage. Such attacks reinforce the importance of protecting the backup environment in the event that the production environment is compromised. Common techniques to achieve this include network segmentation, highly restricted and segregated access controls and network traffic flow restrictions.

Physical and environmental controls

43. The absence of physical and environmental controls can compromise the effectiveness of other information security controls. An APRA-regulated entity would typically have in place the following physical and environmental controls (commonly through professionally managed data centres as part of third party or related party arrangements):

a) location and building facilities that provide a level of protection from natural and man-made threats. This includes diversity of access to key utility services such as power and telecommunications, as well as fall-back mechanisms where access to the key utility service has failed (e.g. generators, Uninterrupted Power Supply (UPS) devices and alternate telecommunication connections);

b) physical access controls that protect the site perimeter, building, data room and computing racks. Common controls include gates, locks and procedures for granting and reviewing access by staff, third party providers and visitors;

c) environmental controls which maintain environmental conditions within acceptable parameters. Common controls include ventilation, air conditioning and fire suppressant systems; and

d) monitoring and alert mechanisms that detect information security incidents where physical and environmental controls have failed. Common controls include sensors/alarms for temperature, humidity, water, smoke, unauthorised access; and service availability alerts (e.g. power supply, telecommunication, servers).

Security in change management

44. APRA envisages that a regulated entity would implement controls to manage changes to information assets, including changes to hardware, software, data, and configuration (both where the change is planned and in response to an emergency) with the aim of maintaining information security. This would typically include:

    a) security testing (including reviews) to identify vulnerabilities and confirm information security requirements have been met. The nature of testing would be commensurate with the scope of the change and the sensitivity and criticality of the impacted information asset (refer to Attachment H for examples of common testing techniques);

    b) approval of changes prior to deployment into the production environment;

    c) segregation of duties in place between personnel who undertake a change and those deploying a change to production;

    d) changes are developed and verified in another environment,[7] sufficiently segregated from production so as to avoid any compromise of information security;

    e) information security requirements are validated prior to deployment;

    f) desensitising sensitive production data when used for development or testing purposes; and

    g) intentionally introduced information security vulnerabilities are authorised. In APRA's view, changes that knowingly introduce security vulnerabilities would be minimised and, where possible, compensating controls implemented. This situation normally arises when dealing with system outages.

Software security

45. An APRA-regulated entity would typically implement secure software development and acquisition techniques to assist in maintaining confidentiality, integrity and availability by improving the general quality and vulnerability profile of the software (refer to Attachment D for further guidance).

46. The outcome of secure software development and acquisition is to ensure that software:

    a) continues to function as intended regardless of unforeseen circumstances, including where erroneous input is supplied;

    b) has a reduced propensity to be misused either intentionally (e.g. for the purposes of theft) or inadvertently; and

[7] A regulated entity would typically run multiple environments reflecting the various stages of software development and testing (e.g. development, system testing, user acceptance testing, staging).

c) complies with the information security policy framework.

Data leakage

47. Data leakage is the unauthorised removal, copying, distribution, capturing or other types of disclosure of sensitive data that results in a loss of data confidentiality (also known as a data breach). Access to data removal methods would typically be subject to risk assessment and only granted where a valid business need exists.

48. Controls, commensurate with the sensitivity and criticality of the data, would typically be implemented where sensitive data is at risk of leakage. Examples of data leakage methods include the use of portable computing devices (e.g. laptops, tablets, 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.

49. Typically, the strength of data leakage controls would be commensurate with the sensitivity of the data. Common controls include:

    a) authorisation, registration and regular review of users and associated transfer mechanisms and devices, including printers, telephony and video conferencing equipment. Users with a greater level of access to sensitive data would be subject to increased scrutiny;

    b) appropriate blocking, filtering and monitoring of electronic transfer mechanisms, websites and printing;

    c) appropriate encryption, cleansing and auditing of devices;

    d) appropriate segmentation of data, based on sensitivity and access needs;

    e) monitoring for unauthorised software and hardware (e.g. key loggers, password cracking software, wireless access points, business implemented technology solutions); and

    f) appropriate removal of sensitive data after recovery tests are concluded.

50. Wholesale access to sensitive data (e.g. contents of customer databases or intellectual property that can be exploited for personal gain) would be highly restricted to reduce the risk exposure to significant data leakage events. Industry experience of actual data leakage incidents include the unauthorised extraction of debit/credit card details, theft of personally identifiable information, loss of unencrypted backup media and the sale/trade or exploitation of customer identity data.

Cryptographic techniques to restrict access

51. Cryptographic techniques can be used to control access[8] to sensitive data, both in storage and in transit. The strength of the cryptographic techniques deployed would be commensurate with the sensitivity and criticality of the data as well as other supplementary or compensating controls (refer to Attachment E for further guidance).

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

Information security technology solutions

53. An APRA-regulated entity would typically deploy appropriate information security technology solutions which maintain the security of information assets. Examples include firewalls, network access control, intrusion detection/prevention devices, anti-malware, encryption and monitoring/log analysis tools. The degree of reliance placed on technology solutions for information security could necessitate a heightened set of life-cycle controls, including but not limited to:

    a) guidelines outlining when information security-specific technology solutions should be used;

    b) standards documenting the detailed objectives and requirements of individual information security-specific technology solutions;

    c) authorisation of individuals who can make changes to information security-specific technology solutions. This would typically take into account segregation of duties issues;

    d) regular assessment of the information security-specific technology solutions configuration, assessing both continued effectiveness as well as identification of any unauthorised access or modification;

    e) periodic review of industry practice and benchmarking against peers; and

    f) detection techniques deployed which provide an alert if information security-specific technology solutions are not working as designed.

End-user developed/configured software

54. Current technologies allow end-users to develop/configure software for the purpose of automating day-to-day business processes or facilitating decision-making (e.g. spreadsheets, local databases, user administered software). This creates the risk that life-cycle controls could be inadequate for critical information assets and possibly lead to a proliferation of sensitive data being accessible outside controlled environments.

---

[8] Cryptographic techniques may also be used to verify data integrity.

55. An APRA-regulated entity would typically introduce processes to identify and classify end-user developed/configured software and assess risk exposures. In APRA's view, any information software asset that is critical to achieving the objectives of the business or that processes sensitive data would comply with the relevant life-cycle management controls of the regulated entity.

56. Sound practice is to establish a formal policy to govern end-user developed/configured software. The policy would clearly articulate under what circumstances end-user developed/configured software is appropriate, as well as expectations regarding life-cycle management controls including information security, development, change management and backup.

Emerging technologies

57. New technologies potentially introduce a set of additional information security vulnerabilities, both known and unknown. An APRA-regulated entity would typically apply appropriate caution when considering the introduction of new technologies.

58. Typically, an APRA-regulated entity would only authorise the use of new technologies in a production environment where the technology:

    a) has matured to a state where there is a generally agreed set of industry-accepted controls to manage the security of the technology; or

    b) compensating controls are sufficient to reduce residual risk within the entity's risk appetite.

59. An APRA-regulated entity could find it useful to develop a technology authorisation process and maintain an 'approved technology register' to facilitate this. The authorisation process would typically assess the benefits of the new technology against the impact of an information security compromise, including an allowance for uncertainty.

Information assets managed by third parties and related parties

60. Evaluation of the design of information security controls of third parties and related parties necessitates an understanding of the controls in place or planned. This can be maintained over time through a combination of interview, survey, control testing, certifications, contractual review, attestations and independent assurance assessments. Controls identified can then be compared to common industry controls and considered in light of controls within the regulated entity as well as the nature of the information assets involved. Any capability gaps identified would be addressed in a timely manner.

61. Third parties and related party agreements often take advantage of sub-contracting/on-sourcing arrangements, whether at the start of the arrangement or over time. Consequently, in order to effectively evaluate the design of information security controls, an APRA-regulated entity would consider what is permissible within the agreement, and ongoing awareness of changes to the way services are provided.

62. An APRA-regulated institution would usually consider whether information security considerations are appropriately captured in contractual obligations and oversight arrangements. The regulated entity would also consider the scope, depth and independence of any certifications, attestations and assurance provided and take steps to address any limitations identified.

Incident management

Detection of security compromises

63. Under CPS 234, an APRA-regulated entity is required to have robust mechanisms in place to detect and respond to actual or potential compromises of information security in a timely manner. The term 'potential' is used to highlight that information security incidents are commonly identified when an event occurs (e.g. unauthorised access notification, customer complaint) requiring further investigation in order to ascertain whether an actual security compromise has occurred.

64. Detection mechanisms typically include scanning, sensing and logging mechanisms which can be used to identify potential information security incidents. Monitoring processes could include the identification of unusual patterns of behaviour and logging that facilitates investigation and preserves forensic evidence. The strength and nature of monitoring controls would typically be commensurate with the impact of an information security incident. Monitoring processes would consider the broad set of events, ranging from the physical hardware layer to higher order business activities such as payments and changes to user access. Common monitoring techniques include:

    a) network and user profiling that establishes a baseline of normal activity which, when combined with logging and alerting mechanisms, can enable detection of anomalous activity;

    b) scanning for unauthorised hardware, software and changes to configurations;

    c) sensors that provide an alert when a measure breaches a defined threshold(s) (e.g. device, server and network activity);

    d) logging and alerting of access to sensitive data or unsuccessful logon attempts to identify potential unauthorised access; and

    e) users with privileged access accounts subject to a greater level of monitoring in light of the heightened risks involved.

65. Monitoring processes and tools remain in step with the evolving nature of threats and contemporary industry practices.

66. APRA envisages that a regulated entity would establish a clear allocation of responsibilities for monitoring processes, with appropriate tools in place to enable timely detection. Access controls and segregation of duties would typically be used as a means to safeguard the integrity of the monitoring processes.

Response to a security compromise

67. An APRA-regulated entity would maintain plans in line with information security incidents experienced, both internally and externally. Examples of information security incidents include:

    a) malware infection (e.g. virus, ransomware);

    b) data breach (customer or internal data);

    c) compromise of staff or customer credentials (e.g. as the result of a phishing attack);

    d) denial-of-service attack;

    e) hack of an internet-facing platform;

    f) website defacement; and

    g) compromise by an advanced persistent threat.[9]

68. An APRA-regulated entity would typically have clear accountability and communication strategies to limit the impact of information security incidents. Under CPS 234, this includes escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate. A regulated entity could also include customer communication as part of any such communication strategy where appropriate. Incident response plans would also typically assist in compliance with regulatory notification requirements.

69. The level of detail of response plans would be sufficient to minimise the amount of decision-making required and provide clarity regarding roles and responsibilities when experiencing an information security incident.

Information security incident stages

70. Under CPS 234, an APRA-regulated entity's information security response plans must include mechanisms for managing all relevant stages of an incident. These typically include:

    a) detection of an information security event through the use of automated sensors and manual review;

    b) identification and analysis to determine if it is an incident or an event;

[9] Advanced persistent threats (APTs) are characterised as a set of sophisticated, covert and continuous computer hacking processes coordinated by an individual, group or nation-state targeting a specific entity. An APT usually targets organisations or nations for commercial or political motives. APT processes require a high degree of covertness and diligence over a long period of time (typically months).

c) escalation to ensure that decision-makers are aware of the incident and to trigger incident response processes;

d) containment to minimise the damage caused, and reduce the possibility of further damage;

e) eradication which involves the removal of the source of the information security compromise (typically malware);

f) response and recovery which involves a mixture of system restoration (where integrity and availability have been compromised) and managing sensitive data loss where confidentiality has been lost. This allows for a return to business-as-usual processing; and

g) post-incident analysis and review to reduce the possibility of a similar information security incident in the future, improve incident management procedures and forensic analysis to facilitate attribution and restitution (where relevant).

Incident response testing

71. Under CPS 234, an APRA-regulated entity must annually review and test its information security response plans to ensure they remain effective and fit-for-purpose. It is important that the success criteria for such tests are clearly defined, including the circumstances under which re-testing would be required. Test results could be reported to the appropriate governing body or individual, with associated follow-up actions formally tracked and reported.

Third parties and related parties

72. In APRA's view, a regulated entity would benefit from agreeing each party's roles and responsibilities where incident response requires collaboration and coordination between the regulated entity and third parties or related parties. This could involve formalisation of points of integration between third party and related party incident response plans and involvement of third parties and related parties in incident response testing.

73. APRA-regulated entities that place reliance on the information security capabilities of third parties and related parties as part of a broader service provision arrangement would typically seek evidence of the periodic testing of incident response plans by those parties.

Integration with business continuity and crisis management

74. In APRA's view, a regulated entity would benefit from clear linkages between information security response plans and business continuity processes, including crisis management, continuity plans and recovery plans. This could involve integration with third party and related party plans and processes.

Testing control effectiveness

Systematic testing program

75. In order to systematically test information security controls, an APRA-regulated entity would normally outline the population of information security controls across the regulated entity, including any group of which it is a part, and maintain a program of testing which validates the design and operating effectiveness of controls over time. Additional testing could be triggered by changes to vulnerabilities/threats, information assets or the threat landscape.

76. In APRA's view, the frequency and scope of testing would ensure that a sufficient set of information security controls are tested, at least annually, in order to validate that information security controls remain effective. Furthermore, controls protecting information assets exposed to 'untrusted' environments[10] would typically be tested throughout the year.

77. The nature of testing would be a function of the type of control, and would typically consider a variety of testing approaches informed by contemporary industry practices (refer to Attachment G for further guidance).

78. It is important that success criteria for tests are clearly defined, including the circumstances under which re-testing would be required. Test results would be reported to the appropriate governing body or individual, with associated follow-up actions formally tracked and reported.

Independence of testers

79. Under CPS 234, an APRA-regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists. For an APRA-regulated entity to have confidence in the quality of testing, it is important that testers are sufficiently independent in order to provide a bias-free assessment of controls (i.e. unimpeded by a conflict of interest). This includes the use of testers who do not have operational responsibility for the controls being validated. The level of functional independence required would typically be determined by the nature and importance of the testing.

[10] Untrusted environments refers to environments where an APRA-regulated entity is unable to enforce its information security policies, including exposures to the internet and connections to service providers and customers.

Internal audit

Assurance to the Board

80. Internal audit is an important vehicle by which the Board can gain assurance that information security is maintained. This assurance would typically be achieved through the inclusion of information security within the APRA-regulated entity's internal audit plan. The Board could also choose to gain assurance through expert opinion or other means to complement the assurance provided by the internal audit function. This typically occurs where the required skills do not reside within the internal audit function or the area subject to audit pertains to third parties or related parties.

81. Under CPS 234, an APRA-regulated entity's internal audit function must review the design and operating effectiveness of information security controls. In APRA's view an approach which achieves comprehensive assurance would involve an audit program which assesses all aspects of the information security control environment over time. The frequency at which areas to be audited are assessed would take into account the impact of an information security compromise and the ability to place reliance on other control testing undertaken. Additional assurance work may be triggered by changes to vulnerabilities and threats or material changes to IT assets.

82. Where internal audit relies on control testing performed by other areas, APRA would expect the internal audit function to assess the scope and quality of the testing conducted in order to determine how much reliance can be placed upon it.

Use of assurance reports from third parties

83. CPS 234 requires that where reliance is placed on assurance provided by third parties and related parties, internal audit must assess the information security control assurance provided by the third party or related party. Where the assessment identifies deficiencies, or no assurance is available, this would typically be raised with the Board for its consideration.

Notification

Information requirements

84. Under CPS 234, an APRA-regulated entity must notify APRA of certain information security incidents. For this purpose, an APRA-regulated entity would be expected to provide the following information:

    a) name of the APRA-regulated entity;

    b) date and time/period of the incident;

    c) date and time when the incident was assessed as material;

    d) incident type;

    e) incident description;

    f) current status of incident; and

    g) mitigation actions taken or planned (where available).

85. Under CPS 234, an APRA-regulated entity must notify APRA of certain information security control weaknesses. For this purpose, an APRA-regulated entity would be expected to provide the following information:

    a) name of the APRA-regulated entity;

    b) date and time when the control weakness was assessed as material;

    c) control weakness description;

    d) current status of control weakness; and

    e) mitigation actions taken or planned.

86. Material control weakness can be identified through a number of mechanisms. These include control testing, assurance activities, information security incidents (external and internal), vulnerability notification by software and hardware vendors and other forms of notification by third parties and related parties.

Attachment A: Security principles

1. APRA envisages that an APRA-regulated entity would adopt a set of high-level information security principles in order to establish a sound foundation for the entity's information security policy framework. Common information security principles include:

    a) implement multiple layers and types of controls such that if one control fails, other controls limit the impact of an information security compromise. This is typically referred as the principle of 'defence in depth';

    b) access to, and configuration of, information assets is restricted to the minimum required to achieve business objectives. This is typically referred to as the principle of 'least privilege' and aims to reduce the number of attack vectors that can be used to compromise information security;

    c) timely detection of information security incidents. This minimises the impact of an information security compromise;

    d) information security is incorporated into the design of the information system asset. This is typically referred to as secure by design;

    e) use of, and access to, information assets is attributable to an individual, hardware or software, and activity logged and monitored;

    f) error handling is designed such that errors do not allow unauthorised access to information assets or other information security compromises;

    g) assume information assets have an unknown and possibly reduced level of information security control. This is typically referred to as the principle of 'never trust, always identify';

    h) segregation of duties is enforced through appropriate allocation of roles and responsibilities. This reduces the potential for the actions of a single individual to compromise information security;

    i) design controls that enforce compliance with the information security policy framework, thereby reducing reliance on individuals; and

    j) design detection and response controls based on the assumption that preventive controls have failed. This is typically referred as the principle of 'assumed breach'.

Attachment B: Training and awareness

1. An APRA-regulated entity could benefit from developing a training and information security awareness program. This would typically communicate to personnel (staff, contractors and third parties) regarding information security practices, policies and other expectations as well as providing material to assist the Board and other governing bodies to execute their duties. Sound practice would involve tracking training undertaken and testing the understanding of relevant information security policies, both on commencement and periodically.

2. An APRA-regulated entity would regularly educate users, including both internal and third party staff, as to their responsibilities regarding securing information assets. Common areas covered would typically include:

    a) personal versus corporate use of information assets;

    b) email usage, internet usage (including social networking) and malware[11] protection;

    c) physical protection, remote computing and usage of mobile devices;

    d) awareness of common attack techniques targeted at personnel and facilities (e.g. social engineering, tailgating);

    e) access controls, including standards relating to passwords and other authentication requirements;

    f) responsibilities with respect to any end-user developed/configured software (including spreadsheets, databases and office automation);

    g) expectations of staff where bring-your-own-device is an option;

    h) handling of sensitive data; and

    i) reporting of information security incidents and concerns.

3. An APRA-regulated entity would typically require users to adhere to appropriate information security policies pertinent to their roles and responsibilities. At a minimum, all users would typically be required to periodically sign-off on these policies as part of the terms and conditions of their employment or contractual agreements.

[11] Malicious software (malware) is software that is intentionally harmful to a computer system or its user. The term incorporates an ever-growing number of subtypes including viruses, worms, trojans, spyware, bots, ransomware and key loggers.

Attachment C: Identity and access

1. Identity and access management controls would ideally ensure access to information assets is only granted where a valid business need exists, and only for as long as access is required. Access is typically granted to users, special purpose system accounts, and information assets such as services and other software.

2. Factors to consider when authorising access to information assets include: business role, physical location, remote access, time and duration of access, patch and anti-malware status, software, operating system, device and method of connectivity.

3. The provision of access involves the following process stages:

    a) identification — determination of who or what is requesting access;

    b) authentication — confirmation of the purported identity; and

    c) authorisation — assessment of whether access is allowed to an information asset by the requestor based on the needs of the business and the level of information security (trust) required.

4. Regulated entities would typically put in place processes to ensure that identities and credentials are issued, managed, verified, revoked and audited for authorised devices, users and software/processes.

5. The strength of identification and authentication would typically be commensurate with the impact should an identity be falsified. Common techniques for increasing the strength of identification and authentication include the use of strong password techniques (i.e. length, complexity, re-use limitations and frequency of change), utilisation of cryptographic techniques and increasing the number and type of authentication factors used. Authentication factors include something an individual:

    a) knows - for example, user IDs and passwords;

    b) has - for example, a security token or other devices in the person's possession used for the generation of one-time passwords; and

    c) is - for example, retinal scans, hand scans, signature scans, digital signature, voice scans or other biometrics.

6. The following are examples where increased authentication strength is typically required, given the impact should an identity be falsified:

    a) administration or other privileged access to sensitive or critical information assets;

    b) remote access (i.e. via public networks) to sensitive or critical information assets; and

    c) high-risk activities (e.g. third-party fund transfers, creation of new payees).

7. A regulated entity would typically deploy the following access controls:

   a) undertake due diligence processes before granting access to personnel. The use of contractors and temporary staffing arrangements may elevate the risk for certain roles;

   b) implementation of role-based access profiles which are designed to ensure effective segregation of duties;

   c) prohibiting sharing of accounts and passwords (including generic accounts);

   d) changing default passwords and user names;

   e) timely removal of access rights whenever there is a change in role or responsibility and on cessation of employment;

   f) session timeouts;

   g) processes to notify appropriate personnel of user additions, deletions and role changes;

   h) audit logging and monitoring of access to information assets by all users;

   i) regular reviews of user access by information asset owners to ensure appropriate access is maintained;

   j) multi-factor authentication for privileged access, remote access and other high-risk activities;

   k) generation, in preference to storage, of passwords/PINs[12] where used to authorise high-risk activities (e.g. debit/credit card and internet banking transactions); and

   l) two-person rule applied to information assets with the APRA-regulated entity's highest level of sensitivity rating (e.g. encryption keys, PIN generation, debit/credit card databases).

8. For accountability purposes, a regulated entity would typically ensure that users and information assets are uniquely identified and their actions are logged at a sufficient level of granularity to support information security monitoring processes.

[12] 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.

Attachment D: Software security

1. APRA envisages that a regulated entity would formally include information security considerations throughout the software delivery life-cycle[13] including requirements-gathering, selection and configuration (for vendor provided software, including Software as a Service[14]), design and programming (for in-house developed software), testing and implementation phases.

2. Ongoing security of existing software would also typically be considered as part of change management and as new vulnerabilities are identified. Typical factors to consider include:

    a) requirements — information security requirements would be explicitly identified as part of the requirements definition of the software and address potential threats;

    b) design — considerations when designing secure software could include software modularisation; where on the network the software is located; what privileges the software executes under; inclusion of information security features as part of the technical specifications; and the information security standards and guidelines the software specifications are written to;

    c) selection and configuration — considerations when selecting and configuring vendor supplied software include due diligence as to the security testing conducted to identify vulnerabilities (either intended or deliberate); user access management capabilities (e.g. role based, support of segregation of duties); interface vulnerabilities; monitoring capabilities; encryption capabilities to protect sensitive data; ability to obtain and implement information security updates in a timely manner; compliance with the security policy framework; and configuration/implementation of the software which minimises the risk of a security compromise;

    d) standards and guidelines — the body of knowledge for developing secure software would typically be embodied in a set of standards and guidelines. Typically, standards would exist for each programming language, taking into account known vulnerabilities and what is considered to be good practice. 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;

[13] This includes traditional waterfall, agile and hybrid delivery models.

[14] This commonly refers to the provision of software for business users via a cloud platform.

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.

3. An APRA-regulated entity could find it useful to maintain a register of approved software development tools and associated usage. The regulated entity would typically 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.

4. An APRA-regulated entity would typically implement roles, responsibilities and tools for managing the registration and deployment of source code to ensure that information security requirements are not compromised.

Attachment E: Cryptographic techniques

1. Cryptographic techniques refer to methods used to encrypt[15] data, confirm its authenticity or verify its integrity. The following are examples where APRA-regulated entities could deploy cryptographic techniques given the risks involved:

    a) transmission and storage of critical and/or sensitive data in an 'untrusted' environment or where a higher degree of security is required;

    b) detection of any unauthorised alteration of data;

    c) verification of the authenticity of transactions or data; and

    d) protection of customer PINs which are typically used for debit/credit cards and online services.

2. An APRA-regulated entity would typically select cryptographic techniques based on the nature of the activity and the sensitivity and criticality of the data involved. The cryptographic techniques would typically be reviewed on a regular basis to ensure that they remain commensurate with vulnerabilities and threats.

3. APRA envisages that a regulated entity would select encryption algorithms from the population of well-established and proven international standards that have been subjected to rigorous public scrutiny and verification of effectiveness. The length of a cryptographic key would typically be selected to render a brute force attack[16] impractical (i.e. would require an extremely long period of time to breach using current computing capabilities).

4. 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 the security of cryptographic keys. Any compromise of the security of cryptographic keys could, in turn, lead to a compromise of the security of the information assets protected by the cryptographic technique deployed.

5. An APRA-regulated entity would typically deploy, where relevant, controls to limit access to cryptographic keys, including:

    a) use of physically and logically protected devices and environments to store and generate cryptographic keys, generate PINs and perform encryption and decryption.

---

[15] 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.

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

In most cases this would involve the use of Hardware Security Modules[17] (HSMs) or similarly secured devices.

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;

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 would be 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.

[17] Hardware Security Module is a type of secure crypto-processor that provides for the secure generation and storage of cryptographic and other sensitive data.

Attachment F: Customer security

1. Products and services delivered via digital channels can introduce additional information security vulnerabilities which, if exploited, could result in potentially material information security incidents impacting beneficiaries. APRA-regulated entities would typically implement preventative, detective and response controls commensurate with these risks. Common controls include:

    a) authentication controls commensurate with the vulnerability and threats associated with the products and services offered. This could include usage of a second channel notification/confirmation of events (e.g. account transfers, new payees, change of address, access from an unrecognised device);

    b) limits to ensure losses are within risk tolerances (e.g. transfer limits, daily transaction limits);

    c) transaction activity monitoring to detect unusual patterns of behaviour and review of loss event trends which may trigger the need for additional controls (e.g. fraud and theft losses); regular review of customer education and security advice to ensure that it remains adequate and aligned with common industry practice;

    d) documented and communicated procedures for incident monitoring and management of fraud, data leakage and identity theft; and

    e) minimising the collection of sensitive customer information beyond what is relevant to the business activities undertaken. This includes customer information used for the purposes of authentication, such as passwords/PINS.

Attachment G: Testing techniques

Control objective	Example controls and practices	Example testing approaches
Limit access to what has been authorised based on job role and principle of least privilege	Identity & Access Management (IAM), user identification and authentication, physical security, employee awareness and training	Social engineering test
Authenticate users with strength of authentication commensurate with sensitivity of the information asset being accessed	Password policy, system authentication controls	Audits of user access
Protect networks from unauthorised network traffic	Firewalls, routers, network segmentation	Penetration tests
Protect systems from malicious attacks	Anti-malware, web and email filtering	Malware test samples, configuration testing
Protect system-to-system communication, including exchange of data, from unauthorised access and use	Encryption, key management	Key management review
Timely detection of unauthorised access and use	Logs, Security Information and Event management (SIEM), security cameras, Intrusion Detection Solutions (IDS), integrity change detection solutions, event analysis and escalation procedures	Penetration tests[18]
Implement secure software	Secure software development, software procurement and deployment practices	Design reviews, penetration tests, code review and scanning, network traffic analysis, fault testing, fuzzing

[18] For the purposes of this document, the term penetration testing includes more advanced techniques commonly referred to as "red team" tests.

Control objective	Example controls and practices	Example testing approaches
Orderly response to information security incidents	Information security incident response playbooks, crisis management, Business Continuity Plans (BCP)	Table top exercises, public-private scenario test
Resilience of systems to handle failure of individual components	Active-active, active-passive solutions deployed, sandboxed solutions, zero trust architecture	Chaos monkey testing, architecture review, fault testing, failover testing
Recovery under all plausible scenarios	Recovery plans, arrangements and tests Controls to protect backups from compromise	Technical recovery tests Backup environment penetration test
Implementation controls minimise risk of new vulnerabilities from system change, systems are secure by design	Secure software development, non-functional testing, change control, system hardening	Change control review, code scanning, architecture review, fuzzing
Timely identification and remediation of new vulnerabilities	Patching, configuration management	Vulnerability scans, penetration testing
Timely identification and remediation of new threats	Threat intelligence, information security strategy	Independent capability review
Inform decision-makers of the sufficiency of information security and direct activity as appropriate	Reports, governance forums, internal audit, independent assurance, consulting reviews	Governance reviews

Attachment H: Reporting

The following tables represents examples of information that could be provided to the Board and management as part of their oversight of information security. APRA-regulated entities could use the contents to assess the completeness of their current reporting mechanisms, as considered appropriate.

Common information reported to Boards and management	
Capability	• Information security strategy, key initiatives and progress to date • Situational awareness analysis (including threat intelligence) • Capability assessments (self-assessed or via benchmarking) • Identified capability gaps and status of remediation activities
Incidents	• Post incident reports for material incidents • Incident trend analysis (internal and external) • Incident response test results (includes simulations)
Controls	• Control testing activities (including schedule, scope, results and trends) • Internal audit activities (including schedule, scope, results and trends) • Progress on risk and remediation activities • Outcomes of vulnerability and threat assessments • Third party and related party assessments • Information security policy framework compliance reporting
Education	• Informational and awareness material • Results of training and awareness sessions

Common metrics reported to Boards and management		
Pre compromise	Events	• External scanning blocked connections (count) • New vulnerabilities (by OWASP[19] type, count) • Malware stopped (count) • Phishing sites known (count) • Phishing site takedown (count, hours open) • Unique malware targeting bank (count) • Vulnerabilities per line of code (count) • Applications going into production with code vulnerabilities (count) • Security events detected (count)
	Practices	• Penetration testing (by type, count and finding rating) • Systems protected by identity and access management systems (count) • Internally developed systems which cannot be updated (by type, count) • Systems with out of vendor support components (by type, count, coverage %) • Systems without anti malware solutions (count) • Non-authorised (compliant) devices (by type, count) • Information security configuration compliance (coverage %) • Awareness exercises (coverage %, count) • Staff responding to phishing tests (% of total staff) • User access review (by role, privilege, ageing, coverage %) • Security assessments of providers over twelve months (% coverage of relevant third parties) • Patch aging (by criticality, days) • Assurance report on information security (findings by rating, ageing to remediation)
On compromise	Events	• Detected malicious software endpoints (count) • Detected malicious software on servers (count) • Online directories containing staff/customer info (count) • Incident type over period (count, by type: denial of service, malicious code, misuse, reconnaissance, social engineering, unauthorised access, other)
	Practices	• Response and recovery plans developed (by type, count, % coverage) • Incident rehearsals (by type, count, % coverage)
Post compromise	Events	• Detected APT (count) • Blocked connections to malicious websites (count) • Data breaches detected (count) • Regulated entity losses ($) • Customer losses ($)
	Practices	• Post incident reports (count)

[19] Open Web Application Security Project (OWASP) is an online community which maintains a categorisation scheme which can be used to categorise vulnerabilities.

APRA