PRO-26: CPS 234 - SUMMARY REPORT

PROGRAM SUMMARY

2020/02/20

Effective From	2020/01/01	**Standards**	CPS Summary
Effective To	N/A		
Report Date	2020/02/20		

Description

Objectives and key requirements of this Prudential Standard This Prudential Standard aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats. A key objective is to minimize the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related parties or third parties. The Board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security. The key requirements of this Prudential Standard are that an APRA-regulated entity must: a)classify its information assets by criticality and sensitivity to determine the potential impact of an information security incident on the entity and the interests of beneficiaries and other customers; b)clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals; c)implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets, and undertake systematic testing and assurance regarding the effectiveness of those controls; and d)notify APRA of material information security incidents.

Scope

This Prudential Standard applies to all 'APRA-regulated entities' defined and Where an APRA-regulated entity's information assets are managed by a third party, the requirements in this Prudential Standard will apply in relation to those information assets from the earlier of the next renewal date of the contract with the third party or 1 July 2020.

Notes

xMatters continuous its commitment to compliance and transparency!

In our continuous efforts to improve and implement controls and safeguards for our clients, xMatters has undergone self-assessment to affirm our compliance with the latest Prudential Standard CPS 234 Information Security introduced by the Australian Prudential Regulation Authority (APRA).

The Prudential Standard CPS 234 Information Security is a federal law for APRA-regulated entities and came into effect on 1 July 2019. The CPS 234 will help the APRA-regulated entities' resilience against information security incidents, and their ability to respond swiftly and effectively in the event of a breach. CPS 234 requires APRA-regulated entities and suppliers to:

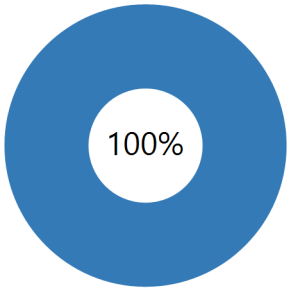
Clearly define information-security related roles and responsibilities;

Maintain an information security capability commensurate with the size and extent of threats to their information assets;

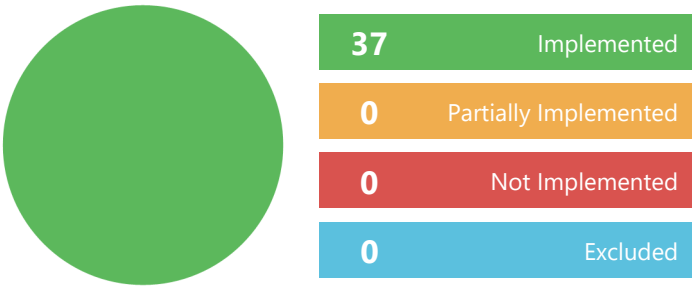
Implement controls to protect information assets and undertake regular testing and assurance of the effectiveness of controls; and

Promptly notify APRA of material information security incidents.

Overall Progress



Implementation Status



Total Controls/Policies

23

Number of Requirements

37

Requirements Per Standard

Requirement	Status	Owner
CPS SUMMARY		
(No Category)		
1.1	Implemented	Information Assurance Department

Information security capability
15. An APRA-regulated entity must maintain an information security capability commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.

Satisfied By

- **Policy:** P-1: Information Security Objectives (Doc 62)
- **Policy:** Security at xMatters
- **Policy:** ISMS Policy

Notes

Our Priority is Data Security

We are committed to providing our clients with a secure environment using the most advanced technologies to safeguard their information. The xMatters Information Security Management System (ISMS) is a guarantee of a great service and a secure platform, where data is treated as a valuable asset and always kept private.

The xMatters security framework is governed by ISO/IEC 27001:2013 Information Security Standard and uses the comprehensive set of policies, processes, and controls for standardized treatment of data. All controls are centrally monitored and assessed for quality assurance.

xMatters has a constantly improving security program in place with semi-annual internal audits conducted by an independent third party, and an external annual certification audit performed by an accredited organization.

Organizational security

- Documented onboarding process and access control for employees
- Employee background checks
- Information security training and awareness programs
- Separation between development and production environments
- Centralized endpoint protection, firewall, and VPN
- Documented and monitored processes for incident management, data breach, risk assessment, nonconformities to the ISMS, and corrective action
- Policies, procedures and controls implemented based on ISO 27001 Information Security
- Management commitment to Information Security objectives and well-established roles and responsibilities
- Management review meetings
- Physical security audits
- Cross-functional team focuses on the application infrastructure security
- Centralized governance, risk management, and compliance (GRC) software

More information here.

Platform security

SaaS resides in Google Cloud Platform (GCP)

Encryption in transit and at rest

Available on multiple regions availability zones

Multiple levels of firewalls policy layers for network and data protection

Logging and monitoring capability

Automated configuration assessment

Documented change management procedure applied to the infrastructure

Third-party penetration testing

Security Framework

The xMatters Information Assurance Team manages an Information Security Management System (ISMS) based on ISO 27001.

Our security framework includes:

- Policies, Procedures and Controls
- Asset Management
- Risk Management
- Access Management
- Organizational Security
- Physical Security
- Cryptography
- Operations Security
- Supplier Security
- Business Continuity
- Compliance

1.2 **Implemented** Information Assurance Department

Information security capability

16. Where information assets are managed by a related party or third party, the APRA-regulated entity must assess the information security capability of that party, commensurate with the potential consequences of an information security incident affecting those assets.

Satisfied By

- **Policy:** Supplier Assessment and Monitoring (SOP A15)

Notes

Supplier Management

xMatters uses third-party sub-processors to provide infrastructure services, and to help us provide notifications and other associated services.

Prior to engaging any third-party sub-processor, xMatters Information Assurance Team performs diligence to evaluate their privacy, security, and confidentiality practices, and executes a non-disclosure agreement implementing its applicable confidentiality obligations. The assessment process is repeated annually.

To obtain a complete list of xMatters sub-processors, contactsecurity@xmatters.com.

1.3 **Implemented** Information Assurance Department

Information security capability
17. An APRA-regulated entity must actively maintain its information security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.

Relates To
- **RiskAnalysis:** ISMS Risk Assessment 2019
- **RiskAnalysis:** RA-44: 2018-2019 WhiteHat Analysis
- **RiskAnalysis:** RA-42: 2019 Qualys Analysis

Satisfied By
- **Policy:** P-11: Vulnerability Management Process (A1261)
- **Policy:** P-14: Risk Assessment (SOP 612)

Notes

Data as an asset (Classification and Handling)

At xMatters, data is treated as a valuable asset. Information assets of the organization will be classified based on their relative business value, legal requirements and impact due to loss of confidentiality, availability and integrity of the information asset. The level of security will be identified based on the information classification performed. Customer data is classified at the highest level.

Vulnerability and Penetration testing
xMatters engages independent vendors to conduct application and infrastructure-level vulnerability scanning and penetration testing on the SaaS platform. All findings are logged into a database, risks are identified, assessed, and treated until residual risk comes down to the lowest acceptable level. Results of vulnerability scans and risk assessments are available to users upon request.

Risk Management

xMatters has a Risk Management Procedure in place to identify, assess and treat risks depending on the level of impact and likelihood. After treatment, all risks are re-assessed for residual risk evaluation. Risks are only accepted when they reach the lowest level and no longer represent threats to xMatters system and data assets.

Incident Management

xMatters has an established procedure for responding to potential security incidents. All security incidents are managed by following the non-conformity treatment process:

• Immediate action

• Root-cause analysis and incident classification (based on severity)

• Corrective action

• Preventive action

All process is documented and updated annually. Lessons learned are kept for future reference.

In the event of an incident, affected customers will be informed by our Technical Support Team or Customer Success Manager.

2.1 **Implemented** Information Assurance Department

Policy framework
18. An APRA-regulated entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.

Satisfied By
- **Policy:** ISMS Policy

Notes

Our Priority is Data Security

We are committed to providing our clients with a secure environment using the most advanced technologies to safeguard their information. The xMatters Information Security Management System (ISMS) is a guarantee of a great service and a secure platform, where data is treated as a valuable asset and always kept private.

The xMatters security framework is governed by ISO/IEC 27001:2013 Information Security Standard and uses the comprehensive set of policies, processes, and controls for standardized treatment of data. All controls are centrally monitored and assessed for quality assurance.

xMatters has a constantly improving security program in place with semi-annual internal audits conducted by an independent third party, and an external annual certification audit performed by an accredited organization.

We've summarized our key security practices below. If you have any questions, contact us at security@xmatters.com.

Organizational security

- Documented onboarding process and access control for employees
- Employee background checks
- Information security training and awareness programs
- Separation between development and production environments
- Centralized endpoint protection, firewall, and VPN
- Documented and monitored processes for incident management, data breach, risk assessment, nonconformities to the ISMS, and corrective action
- Policies, procedures and controls implemented based on ISO 27001 Information Security
- Management commitment to Information Security objectives and well-established roles and responsibilities
- Management review meetings
- Physical security audits
- Cross-functional team focuses on the application infrastructure security
- Centralized governance, risk management, and compliance (GRC) software

More information here.

Platform security

- SaaS resides in Google Cloud Platform (GCP)
- Encryption in transit and at rest
- Available on multiple regions availability zones
- Multiple levels of firewalls policy layers for network and data protection
- Logging and monitoring capability
- Automated configuration assessment
- Documented change management procedure applied to the infrastructure
- Third-party penetration testing

Security Framework

The xMatters Information Assurance Team manages an Information Security Management System (ISMS) based on ISO 27001.

Our security framework includes:

- Policies, Procedures and Controls
- Asset Management
- Risk Management
- Access Management
- Organizational Security
- Physical Security
- Cryptography
- Operations Security
- Supplier Security
- Business Continuity
- Compliance

Security is the responsibility of all xMatters personnel. The entire team is regularly trained, and our systems and processes are audited at planned intervals. The Privacy Officer and the Information Assurance Manager define and maintain the security portfolio up-to-date. The ISMS Steering Committee reviews the entire program and controls on a regular basis during the Management Review Meetings.

2.2 **Implemented** Information Assurance Department

Policy framework
19. An APRA-regulated entity's information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security.

Satisfied By

- **Policy:** ISMS Policy
- **Control:** ISMS Roles and Responsibilities

Notes

xMatters has strict controls in place for administration of the SaaS application by xMatters support engineers. xMatters Access Control model is based on Mandatory Access Control (MAC) using Role Based Access Control (RBAC) to create separation of state.

Users are only provided with access to the network, systems, applications, and network services that they have been specifically authorized to use. Access to the system is audited semi-annually, logged, and verified.

To further reduce the risk of unauthorized access to data, xMatters Access Control model is based on role based access control to create separation of state. There is continuous monitoring at the application and infrastructure level with all monitoring data sent to an event management system. Principles of least privilege are enforced.

xMatters employs multi-factor authentication for all access to systems with client data. Whenever possible, xMatters uses private keys for authentication, in addition to the multi-factor authentication on a separate device. Clients can also use Federated Access Control; xMatters uses Security Assertion Markup Language (SAML) version 2.0 protocol for Identity Provider (IDP) Single Sign-On (SSO).

All employees are required to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks. To manage access to these accounts an authentication tool is used.

3 **Implemented** Information Assurance Department

Information asset identification and classification
20. An APRA-regulated entity must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity. This classification must reflect the degree to which an information security incident affecting an information asset has the potential to affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers.

Satisfied By
- **Policy:** P-3: Information Security Code of Practice
- **Control:** C-27: Inventory of Assets

Notes
At xMatters, data is treated as a valuable asset. Information assets of the organization will be classified based on their relative business value, legal requirements and impact due to loss of confidentiality, availability and integrity of the information asset. The level of security will be identified based on the information classification performed.

Customer data is classified at the highest level.

4.1 **Implemented** Information Assurance Department

Implementation of controls
21. An APRA-regulated entity must have information security controls to protect its information assets, including those managed by related parties and third parties, that are implemented in a timely manner and that are commensurate with:

Satisfied By
- **Policy:** Security at xMatters
- **Control:** Trust Portal

Notes

xMatters Information Assurance Team has documented process to support the APRA-regulated entity to find, assess and mitigate risks, and proactively manage security controls xMatters platform. The Risk Management Analyst analyses an organisation's security based on regular activities and security xMAtters SaaS, providing clients with comprehensive reports that will enable them to monitor xMatters security practices.

For more information, click HERE.

04.1.1 **Implemented** Information Assurance Department

Implementation of controls
(a) vulnerabilities and threats to the information assets;

Satisfied By
- **Policy:** P-11: Vulnerability Management Process (A1261)

Notes
xMatters engages independent vendors to conduct application and infrastructure-level vulnerability scanning and penetration testing on the SaaS platform. All findings are logged into a database, risks are identified, assessed, and treated until residual risk comes down to the lowest acceptable level. Results of vulnerability scans and risk assessments are available to users upon request.

04.1.2 **Implemented** Information Assurance Department

Implementation of controls
(b) the criticality and sensitivity of the information assets;

Satisfied By
- **Policy:** P-3: Information Security Code of Practice
- **Policy:** P-21: Privacy Code of Practice
- **Control:** Encryption (At Rest and in Transit)

Notes

Data Encryption
Data in Transit: xMatters' cryptography controls use Hyper-Text Transfer Protocol Secure (HTTPS) over Transport Layer Security (TLS) version 1.2 using 2048 bit key length, and Internet Protocol Secure (IPSec).
Data at Rest: xMatters uses Data at Rest Encryption using GCP Key Management Service (KMS). All data is encrypted using 256-bit Advanced Encryption Standard (AES-256), with each encryption key is itself encrypted with a regularly rotated set of master keys. xMatters is the only entity that possess the keys for the Data at Rest Cryptographic Controls within GCP and therefore Google does not have access to the data. Each client database protected using schema separation.

Client Data Protection
Data as an asset (Classification and Handling)
At xMatters, data is treated as a valuable asset. Information assets of the organization will be classified based on their relative business value, legal requirements and impact due to loss of confidentiality, availability and integrity of the information asset. The level of security will be identified based on the information classification performed.

Customer data is classified at the highest level.

04.1.3 **Implemented** Information Assurance Department

Implementation of controls
(c) the stage at which the information assets are within their life cycle; and

Satisfied By
- **Control:** Encryption (At Rest and in Transit)
- **Control:** Systems Development Life Cycle (SDLC)
- **Control:** Inventory of Assets - Hardware
- **Control:** C-29: Data Map

Notes
Data Governance

xMatters Data Governance Program includes the following framework:

Administrative, technical and physical controls necessary to protect data.
Policies, Processes, principles, and guidelines.
Applicable Privacy regulations
Stakeholder Accountability: Roles and Responsibilities.

The program is guided by the Data lifecycle: Collection, processing, storing, retention and deletion.

04.1.4 **Implemented** Information Assurance Department

Implementation of controls
(d) the potential consequences of an information security incident.

Satisfied By
- **Policy:** P-18: Breach response Process

Notes
Continuity management is a risk based approach to managing issues that can cause disruption to business operations or service delivery operations.
xMatters manages these risks by determining the most common causes if interruption/disruption and have prepared plans for treatment of these issues.

Within xMatters, the specific roles are identified in relation to continuity management endeavors. Each role has a defined responsibility.

xMatters Business continuity plans are effectively implemented by:

Having all stakeholders briefed on the contents of the BCP and aware of their individual responsibilities;
GCP to be tested and audit results discussed during Management Meetings; and,
Failover tests updated at regular intervals.

Recovery Time Objective & Recovery Point Objective
For contracted purposes, xMatters Recovery Time Objective (RTO) is 30 minutes for business process and support activities recovery.

xMatters Recovery Point Objective (RPO) is 24 hours for contracted purposes based on client data in the Cloud Based Software as a Services (SaaS) instance undergoing full backup once per 24 hours.

4.2 **Implemented** Information Assurance Department

Implementation of controls
22. Where an APRA-regulated entity's information assets are managed by a related party or third party, the APRA-regulated entity must evaluate the design of that party's information security controls that protects the information assets of the APRA-regulated entity.

Satisfied By
- **Policy:** Supplier Assessment and Monitoring (SOP A15)

Notes
xMatters uses third-party sub-processors to provide infrastructure services, and to help us provide notifications and other associated services.
Prior to engaging any third-party sub-processor, xMatters Information Assurance Team performs diligence to evaluate their privacy, security, and confidentiality practices, and executes a non-disclosure agreement implementing its applicable confidentiality obligations. The assessment process is repeated annually.

5.1 **Implemented** Information Assurance Department

Incident management
23. An APRA-regulated entity must have robust mechanisms in place to detect and respond to information security incidents in a timely manner.

Notes
Business Continuity & Disaster Recovery
Continuity management is a risk based approach to managing issues that can cause disruption to business operations or service delivery operations.
xMatters manages these risks by determining the most common causes if interruption/disruption and have prepared plans for treatment of these issues.

Within xMatters, the specific roles are identified in relation to continuity management endeavors. Each role has a defined responsibility.

xMatters Business continuity plans are effectively implemented by:

Having all stakeholders briefed on the contents of the BCP and aware of their individual responsibilities;
GCP to be tested and audit results discussed during Management Meetings; and,
Failover tests updated at regular intervals.

5.2 **Implemented** Information Assurance Department

Incident management
24. An APRA-regulated entity must maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans).

Satisfied By
- **Policy:** P-17: Nonconformity and Corrective Action (SOP 101)
- **Policy:** P-18: Breach response Process

Notes

Incident Response Process

xMatters maintains a record of security incidents with a description of the incident, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. A complete root-cause analysis is performed.

In the case an incident is identified as a confirmed breach, xMatters Service is used to trigger an internal notification to all main stakeholder, that must review the case, immediately.

Notification to affected individuals will be made without undue delay and, in any event, within 72 hours.

5.3 **Implemented** Information Assurance Department

Incident management
25. An APRA-regulated entity's information security response plans must include the mechanisms in place for:

Satisfied By
- **Policy:** P-18: Breach response Process
- **Policy:** P-17: Nonconformity and Corrective Action (SOP 101)

Notes

05.3.1 **Implemented** Information Assurance Department

Incident management
(a) managingall relevant stages of an incident, from detection to post-incident review; and

Notes
An Information security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by us. Good faith acquisition of personal information by an employee or agent of our company for business purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure. An information security breach may also be caused by any individual or software attempt to subvert xMatters access control policies and access client or corporate data without authorization.

Identification and escalation
Preliminary Assessment and Risk Level Assessment
Corrective Action
Automated Escalation Process
Notification
Communication Plan
Support for Affected Individuals
Breach documentation
Review the incident and act to prevent future breaches (Lessons Learned)
Developing a prevention plan

05.3.2 **Implemented** Information Assurance Department

Incident management
(b) 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.

Satisfied By
- **Policy:** P-18: Breach response Process
- **Policy:** P-17: Nonconformity and Corrective Action (SOP 101)

Notes
An Information security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by us. Good faith acquisition of personal information by an employee or agent of our company for business purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure. An information security breach may also be caused by any individual or software attempt to subvert xMatters access control policies and access client or corporate data without authorization.

Identification and escalation
Preliminary Assessment and Risk Level Assessment
Corrective Action
Automated Escalation Process
Notification
Communication Plan
Support for Affected Individuals
Breach documentation
Review the incident and act to prevent future breaches (Lessons Learned)
Developing a prevention plan

5.4 **Implemented** Information Assurance Department

Incident management
26. An APRA-regulated entity must annually review and test its information security response plans to ensure they remain effective and fit-for-purpose.

Notes
xMatters performs yearly review of its policies and procedures.

6.1 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
27. An APRA-regulated entity must test the effectiveness of its information security controls through a systematic testing program. The nature and frequency of the systematic testing must be commensurate with:

Satisfied By
- **Policy:** P-11: Vulnerability Management Process (A1261)

Notes
Assurance Process
Audits
xMatters is in the process to be ISO 27001 certified and is about to initiate engagement for SOC 2 Type II report. In the meantime, an internal audit program was implemented for continuously monitoring, and improving the effectiveness of our security controls and compliance to privacy regulations. These activities are regularly performed by independent external assessors, authorized certification suppliers, and by xMatters Information Assurance Team. Audit results are discussed during management review meetings and all findings are tracked to resolution.

Vulnerability and Penetration testing
xMatters engages independent vendors to conduct application and infrastructure-level vulnerability scanning and penetration testing on the SaaS platform. All findings are logged into a database, risks are identified, assessed, and treated until residual risk comes down to the lowest acceptable level. Results of vulnerability scans and risk assessments are available to users upon request.

06.1.1 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
(a) the rate at which the vulnerabilities and threats change;

Notes

06.1.2 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
(b) the criticality and sensitivity of the information asset;

Notes

06.1.3 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
(c) the consequences of an information security incident; and

Notes

Incident Management

xMatters has an established procedure for responding to potential security incidents.

All security incidents are managed by following the non-conformity treatment process:

- Immediate action
- Root-cause analysis and incident classification (based on severity)
- Corrective action
- Preventive action

All processes are documented and updated annually. Lessons learned are kept for future reference.

In the event of an incident, affected customers will be informed by our Technical Support Team or Customer Success Manager.

06.1.4 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
(d) the risks associated with exposure to environments where the APRA-regulated entity is unable to enforce its information security policies; and

Satisfied By
- **Control:** Service Level Agreements (SLA)
- **Control:** Data Processing agreement

Notes

xMatters contract terms add the ability to examine the service more deeply to meet regulatory requirements.

06.1.5 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
(e) the materiality and frequency of change to information assets.

Satisfied By
- **Policy:** P-3: Information Security Code of Practice

Notes
All controls and documented processes are reviewed on a regular basis.

6.2 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
28. Where an APRA-regulated entity's information assets are managed by a related party or a third party, and the APRA-regulated entity is reliant on that party's information security control testing, the APRA-regulated entity must assess whether the nature and frequency of testing of controls in respect of those information assets is commensurate with paragraphs 27(a) to 27(e) of this Prudential Standard.

Notes

xMatters adheres to the Transparency Principle and make available to clients all necessary information, in order they can properly manage privacy and security practices.

6.3 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
29. An APRA-regulated entity must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner.

Satisfied By
- **Control:** Risk Management Meetings

Notes

xMatters management and stakeholders are updated regularly.

Risk Management Meetings are conducted regularly, controls and processes are reviewed for Optimized maturity level.

6.4 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
30. An APRA-regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists.

Notes
Supplier Management
xMatters uses third-party sub-processors to provide infrastructure services, and to help us provide notifications and other associated services.
Prior to engaging any third-party sub-processor, xMatters Information Assurance Team performs diligence to evaluate their privacy, security, and confidentiality practices, and executes a non-disclosure agreement implementing its applicable confidentiality obligations. The assessment process is repeated annually.

To obtain a complete list of xMatters sub-processors, contactsecurity@xmatters.com

6.5 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
31. An APRA-regulated entity must review the sufficiency of the testing program at least annually or when there is a material change to information assets or the business environment.

Satisfied By
- **Control:** Internal Audit Report

Notes

Audits

xMatters Security framework is audited. At least, semi-annually.

The organization's privacy framework is audited annually against the most restrictive privacy regulations.

6.6 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
32. An APRA-regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties (information security control assurance).

Satisfied By
- **Control:** Internal Audit Report

Notes

6.7 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
33. An APRA-regulated entity must ensure that the information security control assurance is provided by personnel appropriately skilled in providing such assurance.

Satisfied By
- **Control:** ISMS Roles and Responsibilities

6.8 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
34. An APRA-regulated entity's internal audit function must assess the information security control assurance provided by a related party or third party where:

Satisfied By
- **Policy:** Internal Audit (SOP 92)

Notes

06.8.1 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
(a) an information security incident affecting the information assets has the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; and

06.8.2 **Implemented** Information Assurance Department

Testing control effectiveness&Internal Audit
(b) internal audit intends to rely on the information security control assurance provided by the related party or third party.

Notes
Assurance Process
Audits
xMatters is in the process to be ISO 27001 certified and is about to initiate engagement for SOC 2 Type II report. In the meantime, an internal audit program was implemented for continuously monitoring, and improving the effectiveness of our security controls and compliance to privacy regulations. These activities are regularly performed by independent external assessors, authorized certification suppliers, and by xMatters Information Assurance Team. Audit results are discussed during management review meetings and all findings are tracked to resolution.

7.1 **Implemented** Information Assurance Department

APRA notification
35. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 72 hours, after becoming aware of an information security incident that:

Satisfied By
- **Policy:** P-18: Breach response Process

07.1.1 **Implemented** Information Assurance Department

APRA notification
(a) materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries or other customers; or

07.1.2 **Implemented** Information Assurance Department

APRA notification
(b) has been notified to other regulators, either in Australia or other jurisdictions.

Satisfied By
- **Control:** C-25: Authorities List (A613)

7.2 **Implemented** Information Assurance Department

APRA notification

36. An APRA-regulated entity must notify APRA as soon as possible and, in any case, no later than 10 business days, after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.

Notes

xMatters has a process in place to notify the APRA-regulated entity of an information security incident. The APRA-regulated entity when "becomes aware" of an incident must notify APRA as soon as possible and, in any case, no later than 72 hours, after receiving notice from xMatters and evaluating whether the incident requires APRA notification under the criteria in section 35.