Meeting the Requirements of CPS 230 & CPS 234

A guide for APRA-regulated entities

July 2025
AUSTRALIA
Prudential Standard CPS 230
Operational Risk Manageme
Objectives and key requiremen
Standard
AUSTRALIA
Prudential Standard CPS 234
Information Security
Objectives and key requirements of this Standard

This Prudential Standard aims to ensure that an APRA-regulated measures to be resilient against information security incidents (attacks) by maintaining an information security capability com information security vulnerabilities and threats.

A key objective is to minimise the likelihood and impact of incidents on the confidentiality, integrity or availability of including information assets managed by related parties

The Board of an APRA-regulated entity is ultimatel the entity maintains its information security.

The key requirements of this Prudential S

Camms.

Software to Change Tomorrow.

New Standards for APRA-Regulated Entities

APRA have introduced 2 new standards that will become mandatory for all APRA-regulated entities serving the Australian financial services sector from 1st July 2025.

CPS 230 Operational Risk Management

According to APRA, to comply with CPS 230 organisations must:

Risk Management & Controls

Identify, assess and manage its operational risks, with effective internal controls, monitoring and remediation.

Business Continuity

Be able to continue to deliver its critical operations within tolerance levels through severe disruptions, with a credible business continuity plan (BCP).

Third-party Risk Management

Effectively manage the risks associated with service providers, with a comprehensive service provider management policy, formal agreements and robust monitoring.

CPS 234 Information Security

According to APRA, to comply with CPS 234 organisations must:

Define Roles

Clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals.

IT & Cyber Risk Management

Maintain an information security capability appropriate to the size and extent of threats to the organisations' information assets - which enables the continued sound operation of the entity.

Cybersecurity Controls

Implement controls to protect the firms' information assets - commensurate with the criticality and sensitivity of those information assets - and undertake systematic testing and assurance regarding the effectiveness of those controls.

APRA Notification

Notify APRA of material information security incidents and control weaknesses.

Why were these 2 new standards introduced?

The financial services sector forms part of our critical infrastructure and to safeguard the financial interests of people and businesses APRA have introduced 2 new standards. CPS 230 has been introduced to ensure that APRA-regulated entities are resilient to operational risks and disruptions. CPS 234 is designed to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyberattacks) and to minimise the likelihood and impact of information security incidents.

Which organisations need to comply with the new standards?

- **Authorised Deposit-Taking Institutions (ADIs)** including banks, credit unions, and building societies.
- **Insurers** including general insurers (property and casualty insurance companies), life insurers (providers of life insurance and related products) and private health insurers (private health insurance coverage).
- **Registered Superannuation Entity (RSE) Licensees**
- **Authorised/Registered Non-Operating Holding Companies** which hold controlling interests in APRA-regulated entities.

What processes does my organisation need to implement to comply with the new standards?

CPS 230

- Operational Risk Management
- Internal Controls
- Risk Monitoring & Remediation
- Incident Management
- Business Continuity Planning
- Third Party Risk Management

CPS 234

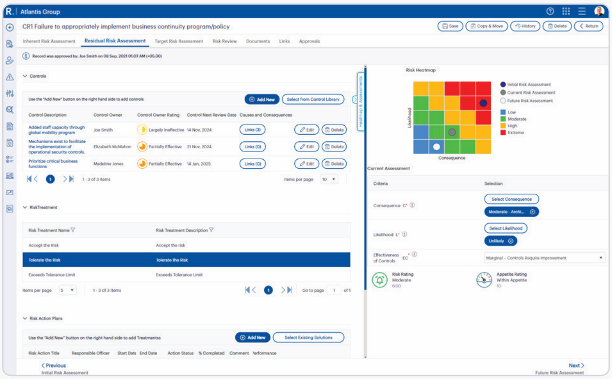
- Cyber & IT Risk Management
- Cyber Incident Reporting
- Information Security Controls
- Information Security Policies
- Establish Cyber Roles & Responsibilities
- APRA Notification Process

How can the Camms platform support organisations to align their processes with CPS 230 & CPS 234?

Risk Management

Set up a best-practice risk management programme to identify, track and reduce operational risk.

- ✓ Create online risk registers with predefined frameworks to categorise & rate risk and establish clear ownership.
- ✓ Roll out risk assessments, surveys, and tasks online - with all data feeding directly into the tool.
- ✓ Pull data into the tool from other systems & sources via APIs to monitor risk.
- ✓ Use automated workflows to approve and escalate risk and implement detailed risk treatment plans.
- ✓ View comprehensive dashboards & reports for risk.



CR1 Failure to appropriately implement business continuity program/policy

Record was approved by: Joe Smith on 08 Sep, 2021 01:07 AM (+05:30)

Use the "Add New" button on the right hand side to add controls

Control Description	Control Owner	Control Owner Rating	Control Next Review Date	Causes and Consequences	
Added staff capacity through global mobility program	Joe Smith	Largely Ineffective	14 Nov, 2024	Links (3)	Edit Delete
Mechanisms exist to facilitate the implementation of operational security controls.	Elizabeth McMahon	Partially Effective	21 Nov, 2024	Links (0)	Edit Delete
Prioritize critical business functions	Madeline Jones	Partially Effective	14 Jan, 2025	Links (0)	Edit Delete

1 - 3 of 3 items Items per page 10

Risk Treatment Name	Risk Treatment Description
Accept the Risk	Accept the risk
Tolerate the Risk	Tolerate the Risk
Exceeds Tolerance Limit	Exceeds Tolerance Limit

Items per page 5 1 - 3 of 3 items Go to page 1 of 1

Use the "Add New" button on the right hand side to add Treatmentss

Risk Action Title	Responsible Officer	Start Date	End Date	Action Status	% Completed	Comment	'erformance

Current Assessment

Criteria	Selection
Consequence C*	Select Consequence Moderate - Archi...
Likelihood L*	Select Likelihood Unlikely
Effectiveness of Controls EC*	Marginal – Controls Require Improvement

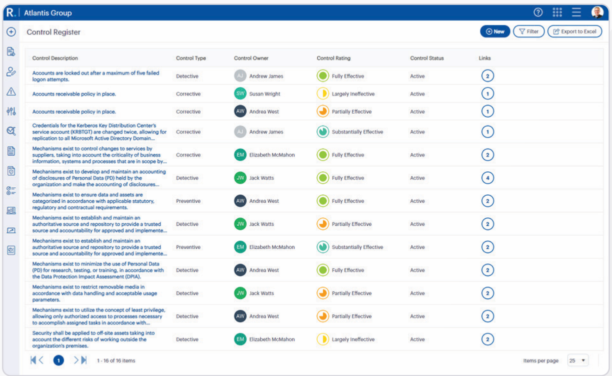
Risk Rating Moderate 6.00

Appetite Rating Within Appetite 10

Controls

Set up a control library to establish controls for the most critical risks.

- ✓ Build a library of relevant controls to operate within your risk appetite.
- ✓ Map controls to the relevant risks in the risk register.
- ✓ Carry out control checks and control testing to ensure controls are effective.
- ✓ Easily identify gaps in your control environment and implement remediating actions.



Control Register

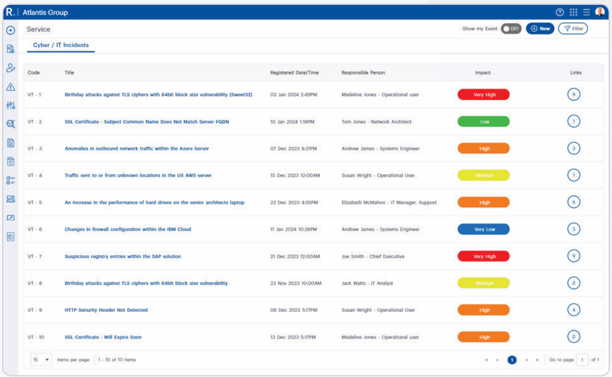
Control Description	Control Type	Control Owner	Control Rating	Control Status	Links
Accounts are locked out after a maximum of five failed logon attempts.	Detective	Andrew James	Fully Effective	Active	2
Accounts receivable policy in place.	Corrective	Susan Wright	Largely Ineffective	Active	1
Accounts receivable policy in place.	Corrective	Andrea West	Partially Effective	Active	1
Credentials for the Kerberos Key Distribution Center's service account (KRBTGT) are changed twice, allowing for replication to all Microsoft Active Directory Domain...	Corrective	Andrew James	Substantially Effective	Active	1
Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business information, systems and processes that are in scope by...	Corrective	Elizabeth McMahon	Fully Effective	Active	2
Mechanisms exist to develop and maintain an accounting of disclosures of Personal Data (PD) held by the organization and make the accounting of disclosures...	Detective	Jack Watts	Fully Effective	Active	4
Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	Preventive	Andrea West	Fully Effective	Active	2
Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemente...	Detective	Jack Watts	Partially Effective	Active	2
Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemente...	Preventive	Elizabeth McMahon	Substantially Effective	Active	2
Mechanisms exist to minimize the use of Personal Data (PD) for research, testing, or training, in accordance with the Data Protection Impact Assessment (DPIA).	Detective	Andrea West	Fully Effective	Active	2
Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	Detective	Jack Watts	Partially Effective	Active	2
Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with...	Detective	Andrea West	Partially Effective	Active	2
Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Detective	Elizabeth McMahon	Largely Ineffective	Active	2

1 - 16 of 16 items Items per page 25

Incident Management

Capture incidents, events and near misses in real-time and manage cases through to resolution.

- ✓ Log incidents online or via the mobile app.
- ✓ Utilise automated workflows for approvals, signoffs, and escalations.
- ✓ Conduct investigations to determine impact and implement controls and treatment actions.
- ✓ Incident reporting portal for vendors & third parties.
- ✓ View dashboards & reports to understand the source of incidents to reduce future occurrences.
- ✓ Map incidents back to the originating risks.



Service

Cyber / IT Incidents

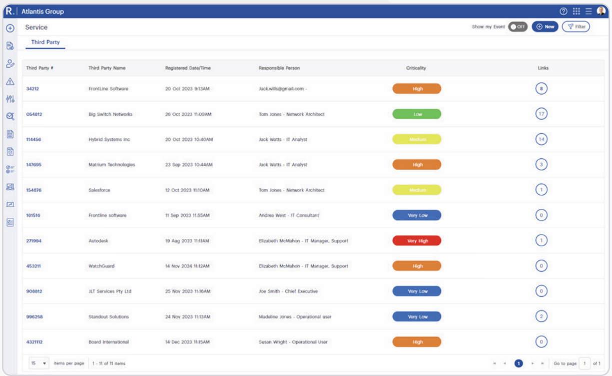
Code	Title	Registered Date/Time	Responsible Person	Impact	Links
VT - 1	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	03 Jan 2024 2:49PM	Madeline Jones - Operational user	Very High	9
VT - 2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	10 Jan 2024 1:18PM	Tom Jones - Network Architect	Low	1
VT - 3	Anomalies in outbound network traffic within the Azure Server	07 Dec 2023 8:21PM	Andrew James - Systems Engineer	High	3
VT - 4	Traffic sent to or from unknown locations in the US AWS server	15 Dec 2023 12:00AM	Susan Wright - Operational User	Medium	1
VT - 5	An increase in the performance of hard drives on the senior architects laptop	23 Dec 2023 4:55PM	Elizabeth McMahon - IT Manager, Support	High	6
VT - 6	Changes in firewall configuration within the IBM Cloud	11 Jan 2024 10:26PM	Andrew James - Systems Engineer	Very Low	3
VT - 7	Suspicious registry entries within the SAP solution	21 Dec 2023 12:00AM	Joe Smith - Chief Executive	Very High	9
VT - 8	Birthday attacks against TLS ciphers with 64bit block size vulnerability	23 Nov 2023 10:00AM	Jack Watts - IT Analyst	Medium	0
VT - 9	HTTP Security Header Not Detected	06 Dec 2023 5:17PM	Susan Wright - Operational User	High	4
VT - 10	SSL Certificate - Will Expire Soon	13 Dec 2023 5:17PM	Madeline Jones - Operational user	High	0

15 items per page 1 - 10 of 10 items Go to page 1 of 1

Camms.

Third-party Risk Management

Ensure the vendors, suppliers and third parties that you depend on are not exposing your organisation to unnecessary risk.



Atlantis Group

Service

Third Party

Show my Event OFF | New | Filter

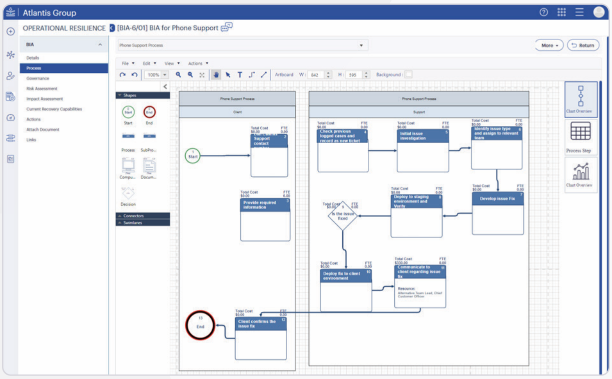
Third Party #	Third Party Name	Registered Date/Time	Responsible Person	Criticality	Links
34212	FrontLine Software	20 Oct 2023 9:13AM	Jack.wills@gmail.com -	High	8
054812	Big Switch Networks	26 Oct 2023 11:09AM	Tom Jones - Network Architect	Low	17
114456	Hybrid Systems Inc	20 Oct 2023 10:40AM	Jack Watts - IT Analyst	Medium	14
147695	Matrium Technologies	23 Sep 2023 10:44AM	Jack Watts - IT Analyst	High	3
154876	Salesforce	12 Oct 2023 11:10AM	Tom Jones - Network Architect	Medium	1
161516	Frontline software	11 Sep 2023 11:55AM	Andrea West - IT Consultant	Very Low	0
271994	Autodesk	19 Aug 2023 11:11AM	Elizabeth McMahon - IT Manager, Support	Very High	1
453211	WatchGuard	14 Nov 2024 11:12AM	Elizabeth McMahon - IT Manager, Support	High	0
908812	JLT Services Pty Ltd	25 Nov 2023 11:16AM	Joe Smith - Chief Executive	Very Low	0
996258	Standout Solutions	24 Nov 2023 11:13AM	Madeline Jones - Operational user	Very Low	2
4321112	Board International	14 Dec 2023 11:15AM	Susan Wright - Operational User	High	0

15 items per page | 1 - 11 of 11 items | 1 | Go to page 1 of 1

- Establish an active online vendor register.
- Roll out vendor risk assessments online via our external facing portal.
- Pull in risk data from third-party intelligence providers.
- Monitor vendor performance against SLAs, KPI's, & scorecards.
- Set controls to reduce vendor risk.
- View dashboards & reports to understand vendor risk exposure.

Business Continuity

Prepare for unexpected disruptions and ensure long term sustainability with a best-practice business continuity plan.



Atlantis Group

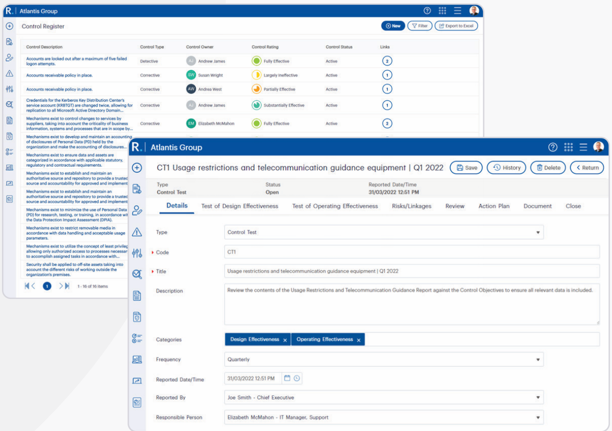
OPERATIONAL RESILIENCE [BIA-6/01] BIA for Phone Support

BIA
Details
Process
Governance
Risk Assessment
Impact Assessment
Current Recovery Capabilities
Actions
Attach Document
Links
Phone Support Process
More
Return
File
Edit
View
Actions
100%
Artboard W: 842 H: 595 Background:
Shapes
Start
End
Process
SubPro...
Compu...
Docum...
Decision
Connectors
Swimlanes
Phone Support Process
Client
Support
Start
Support contact
Provide required information
Check previous logged cases and record as new ticket
Initial issue investigation
Identify issue type and assign to relevant team
Develop issue Fix
Deploy to staging environment and Verify
Is the issue fixed
Deploy fix to client environment
Communicate to client regarding issue fix
Resource: Alternative Team Lead, Chief Customer Officer
Client confirms the issue fix
End
Total Cost $0.00
FTE 0.00
Total Cost $330.00
Chart Overview
Process Step
Chart Overview

- Maintain critical business operations during and after a disruption with a best-practice BCM plan.
- Create an online register of all your critical business processes.
- Access best-practice BCM plan templates.
- Perform risk & business impact assessments and dependency mapping & business process modelling.
- Conduct scenario and vulnerability testing.
- View dashboards & reports to identify gaps in your BCM plans.

Cyber & IT Risk Management

Effectively manage cyber risk and ensure accountability for information security.



Atlantis Group

Control Register

New | Filter | Export to Excel

Control Description	Control Type	Control Owner	Control Rating	Control Status	Links
Accounts are locked out after a maximum of five failed logon attempts.	Detective	Andrew James	Fully Effective	Active	2
Accounts receivable policy in place.	Corrective	Susan Wright	Largely Ineffective	Active	1
Accounts receivable policy in place.	Corrective	Andrea West	Partially Effective	Active	1
Credentials for the Kerberos Key Distribution Center's service account (KRBTGT) are changed twice, allowing for replication to all Microsoft Active Directory Domain...	Corrective	Andrew James	Substantially Effective	Active	1
Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business information, systems and processes that are in scope by...	Corrective	Elizabeth McMahon	Fully Effective	Active	2
Mechanisms exist to develop and maintain an accounting of disclosures of Personal Data (PD) held by the organization and make the accounting of disclosures...					
Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.					
Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implement					
Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implement					
Mechanisms exist to minimize the use of Personal Data (PD) for research, testing, or training, in accordance wit the Data Protection Impact Assessment (DPIA).					
Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.					
Mechanisms exist to utilize the concept of least privileg allowing only authorized access to processes necessar to accomplish assigned tasks in accordance with...					
Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.					

1 | 1 - 16 of 16 items

Atlantis Group

CT1 Usage restrictions and telecommunication guidance equipment | Q1 2022

Save | History | Delete | Return

Type: Control Test
Status: Open
Reported Date/Time: 31/03/2022 12:51 PM

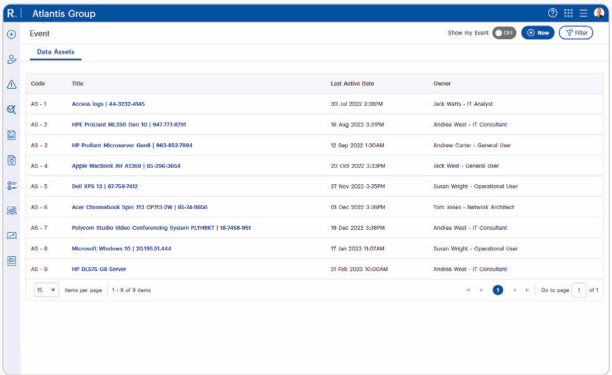
Details | Test of Design Effectiveness | Test of Operating Effectiveness | Risks/Linkages | Review | Action Plan | Document | Close

Type: Control Test
Code: CT1
Title: Usage restrictions and telecommunication guidance equipment | Q1 2022
Description: Review the contents of the Usage Restrictions and Telecommunication Guidance Report against the Control Objectives to ensure all relevant data is included.
Categories: Design Effectiveness ×, Operating Effectiveness ×
Frequency: Quarterly
Reported Date/Time: 31/03/2022 12:51 PM
Reported By: Joe Smith - Chief Executive
Responsible Person: Elizabeth McMahon - IT Manager, Support

- Create an online cyber risk register with predefined frameworks to categorise & rate risk.
- Implement automated monitoring to detect cyber threats and vulnerabilities.
- Implement controls to actively reduce cyber risk.
- Capture and resolve cyber incidents.
- View dashboards & reports to build a holistic view of cyber risk exposure.

Information Security Framework

Establish an information security framework that aligns with CPS 234 requirements.

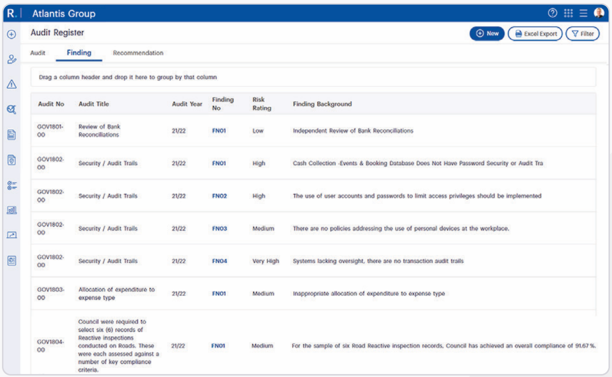


Code	Title	Last Active Date	Owner
AS - 1	Access logs | 44-3232-4145	30 Jul 2022 2:38PM	Jack Watts - IT Analyst
AS - 2	HPE ProLiant ML350 Gen 10 | 947-777-8791	16 Aug 2022 3:31PM	Andrea West - IT Consultant
AS - 3	HP Proliant Microserver Gen8 | 963-852-7894	12 Sep 2022 1:30AM	Andrew Carter - General User
AS - 4	Apple MacBook Air A1369 | 85-296-3654	20 Oct 2022 3:33PM	Jack West - General User
AS - 5	Dell XPS 13 | 87-759-7412	27 Nov 2022 3:35PM	Susan Wright - Operational User
AS - 6	Acer Chromebook Spin 713 CP713-2W | 85-74-9856	01 Dec 2022 3:36PM	Tom Jones - Network Architect
AS - 7	Polycom Studio Video Conferencing System PLYHRKT | 18-7458-951	19 Dec 2022 3:38PM	Andrea West - IT Consultant
AS - 8	Microsoft Windows 10 | 20.195.51.444	17 Jan 2023 11:07AM	Susan Wright - Operational User
AS - 9	HP DL575 G8 Server	21 Feb 2023 10:00AM	Andrea West - IT Consultant

- Build a library of applicable cyber policies & regulations and monitor compliance.
- Manage policy updates, amendments, and attestations.
- Use online registers to classify your data assets and monitor usage.
- Define roles & responsibilities for information security - from operational staff to the board
- Regularly assess information security procedures to ensure they align with your size and threat landscape.

Audit

Manage all you internal and external audits in one centralised platform.

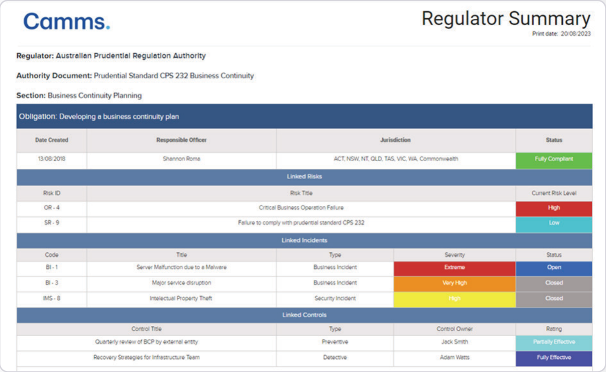


Audit No	Audit Title	Audit Year	Finding No	Risk Rating	Finding Background
GOV1801-00	Review of Bank Reconciliations	21/22	FN01	Low	Independent Review of Bank Reconciliations
GOV1802-00	Security / Audit Trails	21/22	FN01	High	Cash Collection -Events & Booking Database Does Not Have Password Security or Audit Tra
GOV1802-00	Security / Audit Trails	21/22	FN02	High	The use of user accounts and passwords to limit access privileges should be implemented
GOV1802-00	Security / Audit Trails	21/22	FN03	Medium	There are no policies addressing the use of personal devices at the workplace.
GOV1802-00	Security / Audit Trails	21/22	FN04	Very High	Systems lacking oversight, there are no transaction audit trails
GOV1803-00	Allocation of expenditure to expense type	21/22	FN01	Medium	Inappropriate allocation of expenditure to expense type
GOV1804-00	Council were required to select six (6) records of Reactive inspections conducted on Roads. These were each assessed against a number of key compliance criteria.	21/22	FN01	Medium	For the sample of six Road Reactive inspection records, Council has achieved an overall compliance of 91.67 %.

- Build a centralised, searchable audit register to manage all your internal & external audits – including cyber audits and your CPS230 & CPS 234 audits.
- Plan and schedule your upcoming audits and use online forms to capture the findings.
- Use automated workflows to implement corrective actions.
- Dashboards & reports provide a complete overview of audit requirements & findings for regulators.
- Automate notifications for outstanding & overdue actions.

APRA Notification

Establish workflows to notify APRA of information security issues within the designated timeframe.



Regulator Summary

Print date: 20/08/2023

Regulator: Australian Prudential Regulation Authority

Authority Document: Prudential Standard CPS 232 Business Continuity

Section: Business Continuity Planning

Obligation: Developing a business continuity plan

Date Created	Responsible Officer	Jurisdiction	Status
13/08/2018	Shannon Roma	ACT, NSW, NT, QLD, TAS, VIC, WA, Commonwealth	Fully Compliant

Linked Risks

Risk ID	Risk Title	Current Risk Level
OR - 4	Critical Business Operation Failure	High
SR - 9	Failure to comply with prudential standard CPS 232	Low

Linked Incidents

Code	Title	Type	Severity	Status
BI - 1	Server Malfunction due to a Malware	Business Incident	Extreme	Open
BI - 3	Major service disruption	Business Incident	Very High	Closed
IMS - 8	Intelectual Property Theft	Security Incident	High	Closed

Linked Controls

Control Title	Type	Control Owner	Rating
Quarterly review of BCP by external entity	Preventive	Jack Smith	Partially Effective
Recovery Strategies for Infrastructure Team	Detective	Adam Watts	Fully Effective

- Easily run reports to prove compliance with APRA CPS230 and CPS 234.
- APRA regulated entities have a responsibility to report certain information security incidents and control failures to APRA.
- Use automated workflows to notify relevant staff of reportable incidents and control failures based on APRA guidelines.
- Fully document the escalation and notification process - ensuring transparent auditable processes.

Why choose Camms to manage your APRA requirements?

Best-Practice Risk Management

Use the Camms platform to create a best-practice risk management programme to manage operational risk and cyber risk in one automated online solution.

Modern User Interface

The platform is built on the latest technology making it fast, intuitive, and simple to use. We never stop enhancing the platform and regular quarterly updates are used to release all the latest functionality to users.

API Integrations

Pull information into the platform from other data sources via APIs – enabling you to monitor risk based on live company data.

Integrated Cloud-Based Platform

The platform is built from the ground up using single source code enabling complex mapping between risks, controls, incidents, security policies, and APRA requirements.

Rapid Time to Value

Our solutions can be implemented quickly for fast ROI. Our average go-live time is around 3 months and can be even faster for out-of-the-box implementations.

Modular & Scalable

Start out by implementing modules that meet your immediate needs and add more functionality as and when required.

Set Controls

Efficient risk management requires effective controls, use the Camms platform to build a library of controls and carry out control checks and testing.

Highly Secure

The Camms platform is highly secure and has achieved SOC Type 1 & 2, ISO 27001, and cyber essentials certification, and we have implemented many new security features to ensure client data is protected to the highest standards.

Stakeholder Reporting

Easily provide reports on risk exposure and information security status to internal stakeholders and APRA regulators by accessing a wide variety of dashboards and reports.

Highly Configurable

Admins can easily amend reports, workflows, menus, and dropdowns to meet the bespoke needs of the organisation without professional services fees or coding.

Customer Support

Our customer support team is there for you through every step of your implementation to ensure you get the most out of the Camms platform.

Out-of-the-Box

Best-practice frameworks, online forms, templates, automated workflows, and dashboards & reports make the solution easy to set up.

Camms.

Software to Change Tomorrow.

Easily Structure Your Processes to Align with APRA CPS 230 & CPS 234 Requirements

Complying with CPS 230 and CPS 234 will be mandatory for all APRA-regulated entities from 1st July 2025.

Make sure your operational risk management and information security processes align with the new standards with Camms.

Use our GRC platform to effectively manage operational risks, capture and resolve incidents, implement best-practice IT security measures, manage the risk associated with service providers, and implement best-practice business continuity plans – all within one platform.

For more information request a demo.

Learn More

Request Demo

cammsgroup.com