tripwire by HelpSystems

SOLUTION BRIEF

What Is CPS 234 and Who Needs to Comply with It?

Highlights

The Australian Prudential Regulation Authority (APRA) released the Prudential Standard CPS 234 in direct response to the escalating attack landscape in the financial sector. Which entities are responsible for complying with CPS 234? What are the key requirements, and how can companies best prepare for their audits? This brief highlights the essential information you need to know, and maps Tripwire solutions to the individual requirements of CPS 234.

In November 2018, the Australian Prudential Regulation Authority (APRA) released the Prudential Standard CPS 234 in direct response to the escalating attack landscape in the financial sector. APRA has understood these threats to be the direct result of banking services moving to more complex and heavily used digital platforms. The new standard emerged as an offshoot to the Notifiable Data Breach (NDB) scheme, which went into effect in early 2018.

With the advent of online services and new entities such as neobanks, these controls have now become critical. CPS 234 ensures that APRA-regulated entities have implemented sufficient protections to guarantee information security across the computing platform. CPS 234 applies to any entity that is regulated by APRA.

These entities include:

- Banking organizations, neobanks, credit unions, or any other authorized deposit-taking institution (ADI)
- Insurance companies
- Superannuation Funds
- Private health insurance companies
- Non-operating holding companies
- Life insurance companies and friendly societies

CPS 234 is not limited to domestic entities. It is applicable to foreign entities as well, namely foreign ADIs and foreign general and eligible foreign life insurance companies (EFLICs).

CPS 234 commenced July 2019. This means that if an organization's information assets are managed by a third party, they must make sure any new

contracts are CPS 234 compliant. For any existing contracts, organizations were given a one year grace period to move those contracts into compliance.

Who Is Responsible for CPS 234 Compliance?

The responsibility to ensure compliance with CPS 234 ultimately falls on the board of directors of these APRA-regulated entities. This means that the board must ensure that the entity maintains information security in a manner consistent with the size and extent of the threats to its information assets.

What Are the Key Requirements?

Some of the broader requirements of CPS 234 are:

- Identify, implement, and maintain information security controls that are proportional with the threat posed against organizations
- Clearly define information security-related roles and responsibilities
- Implement controls to protect information assets, and undertake regular testing along with assurance of the controls implemented
- Timely notification to APRA of material information security incidents

One point worth noting is that Clause 13 of the requirement states that the board of an APRA-regulated entity is ultimately responsible to enforce CPS 234 compliance. This means that APRA have recognized information security to be a business concern, not solely a technology problem. This is critical in defining how these organizations approach the implementation of such controls, as non-compliance is not an option and carries heavy fines and sanctions.

CPS 234 does not prescribe the level of granularity or the classification method to these controls; this is left entirely to the regulated entity to implement and categorize.

These broader requirements can be broken into nine compliance areas:

1. **Roles and Responsibilities:** All regulated entities *must* clearly define roles and responsibilities across all aspects of their information security strategy, starting at the board and senior governance committees.
2. **Information Security Capabilities:** Within an organization, information security capabilities that are directly commensurate with the threat posed to the entity must be implemented and maintained.
3. **Policy Framework:** The entity must define an information security policy framework. This framework will serve to articulate the necessary controls and provide guidance and validation regarding information security.
4. **Information Asset Identification and Classification:** All information assets, hardware or software, must be identified and classified to define their criticality and sensitivity.
5. **Implementation of Controls:** The regulated entity must have information security controls to protect its information assets. These include all assets managed by related third parties, as well.

   These controls include:
   - Addressing vulnerabilities and threats to information assets,
   - Labeling the criticality and sensitivity of information assets,
   - The life-cycle stage of an information asset, and
   - The potential repercussion or consequence of a security breach or incident.
6. **Incident Management:** A clearly defined incident management plan must be established, reviewed, and tested annually.
7. **Testing Control Effectiveness:** Control effectiveness must be regularly tested through a degree of standard assurance processes to provide a degree of assurance that vulnerabilities and threats are duly managed and identified across an information asset's lifecycle.
8. **Internal Audit**
9. **APRA Notification:** APRA must be notified within 72 hours of any incident impacting their information assets. The regulated entity must also notify APRA within 10 business days of any control weakness the organization cannot remediate in a timely manner.

How Can Companies Be Best Prepared for Audits of CPS 234? What Are Some Best Practices for Companies to Consider?

Roles and Responsibilities

Complying with CPS 234 can be daunting, but it need not be. Achieving compliance, as with any other information security framework, will require the appropriate technical controls. The biggest challenge to compliance can be a lack of guidelines as well as practical application when dealing with third parties.

There's a lot to do to comply with CPS 234. The easiest requirement to fulfill is to ensure roles and responsibilities of all security staff are clearly defined, articulated, and communicated organization-wide. This simple requirement is not dependent on any technology or strategy, and it is something most organizations tend to achieve by default. Bear in mind that roles and responsibilities need to be articulated for third-party vendors as well and stipulated in their contracts.

APRA Notification

Point Nine of the regulation mandates that organizations must have a streamlined process of notifying APRA of an incident impacting their information assets. The scope of the incident as well as the extent can be determined in parallel. Often, an assessment or internal investigation will take place to determine the type of data that's been compromised and whether it contains any customer information. For such requirements, there's a chance this requirement might overlap with other frameworks, such as GDPR or the NDB scheme.

The challenge here would be to assess each incident on its impact and subsequently establish a time threshold

required to report these breaches. Entities also need to establish a chain of command and an internal reporting process for such breaches.

Third-Party Vendor Compliance

Another challenge is to manage and gain visibility on information security features and processes of third-party vendors and how they would correspond to the potential consequences of a security incident.

First and foremost, a contract must be established between the entity and the third-party vendor to ensure these requirements are maintained. If the third-party vendor does not have the appropriate security measures, entities need to consider an effective yet secure way of doing business—either by enforcing controls through their own processes or technologies (limiting access to a network, as an example) or providing guidance to the third party to bring it to an acceptable level of security posture before business can be conducted. Any shortcomings in third-party security controls must be reflected in the master contract.

Policy Framework, Internal Audits, and Implementation of Controls

Perhaps the most challenging and arduous requirement of CPS 234 is to achieve compliance against a policy framework and implementation of controls on information assets. Depending on the scale of an organization's asset map, achieving compliance can become a repetitive, error-prone, and resource-intensive process. Moreover, constant changes to information assets can render them non-compliant quickly. This leads to compliance drift where the entity's information assets deviate from the desired state of compliance due to a lack of central monitoring of configurations and policies.

All these challenges would apply to any financial entity regardless of which compliance framework they adopt, as well as which systems need to be monitored for configuration assessments and vulnerability assessments.

How Tripwire Can Help

Tripwire is synonymous with change monitoring, compliance, configuration assessment, and vulnerability assessment. Besides these capabilities, Tripwire can help entities achieve other aspects of CPS 234, namely being able to discover and identity information assets, supporting internal audit, as well support SOC teams for the purpose of incident management.

As an example, Tripwire Enterprise can help organizations achieve a level of compliance to their adopted policy framework by running scans across

Where Tripwire Can Help Financial Entities Achieve CPS 234 Compliance

AREA	TRIPWIRE ENTERPRISE	TRIPWIRE IP360
Policy Framework	Provides entities the ability to monitor for and comply to adopted policy framework.	
Information Asset Identification and Classification		Provides the ability to identify, classify, and tag assets based on sensitivity and criticality.
Implementation of Controls: Secure Configuration	Provides entities the ability to scan asset configuration and assess against industry best practices, achieving a high degree of system hardening.	
Implementation of Controls: Vulnerability Assessment		Provides the ability to establish a robust vulnerability management process, including regular scanning, identification, risk classification, and remediation of all vulnerabilities.
Testing Control Effectiveness	Allows organizations to validate asset configuration controls by conducting regular technical and configuration assessments against security controls.	
Internal Audit	Aids in internal audit by providing a streamlined and central mechanism to validate all changes, configuration settings, and compliance non-compliances, as well as provide proof of same.	
Information Security Capabilities	Provides context around misconfigurations, data breaches, and identifies threat vectors that can aid in enhancing information security capabilities.	Provides granular visibility on overall risk score of all assets, based on several metrics including business context, age of vulnerability, and ease of exploit to determine priorities in remediation and patching.

their IT assets and documenting where the entity passes or fails to comply with these granular checks. This can be achieved centrally on all IT assets, regardless of being physical, virtual, or cloud-based. Tripwire Enterprise can also help to ensure that entities comply with popular configuration baselines such as CIS or NIST, and that they drastically reduce their attack surface by securely configuring their IT assets. The ability to understand change across all IT assets, enriched by context, allows entities to understand changes across their IT environment to distinguish between good, bad, authorized, and unauthorized changes.

Another requirement that Tripwire can fulfill is to ensure entities can run a robust vulnerability assessment program, providing insights into undetected vulnerabilities before they become an issue. Entities can also tag all discovered assets based on configurable labels around business context, role, sensitivity, and criticality of assets.

The intention and structure of CPS 234 was established to promote and encourage good security practices within financial institutions and to place due responsibility and accountability on the board. However, experience has shown that complying with such guidelines can be cumbersome and daunting when not supported with the right solution and process model.

CPS 234 isn't about enforcement; the intention here is to create a compliant and resilient security posture and at the same time reduce the attack risk surface industry wide. In today's world of an ever-expanding and fast-evolving landscape of the financial sector where crypto- and microbanks have become the new normal, this is a good place to start.

Schedule Your Demo Today

Let us take you through a demo of Tripwire security and compliance solutions, where we'd be happy to answer any of your questions. Visit **tripwire.me/demo**

tripwire® by HelpSystems

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

SBCPS1a 2203