FirmGuard
SECURITY ANALYTICS

APRA Prudential Standard CPS 234

All APRA-regulated entities are expected to meet the new requirements for Prudential Standard CPS 234 Information Security by July 1st 2019.

CPS 234 is intended to shore up APRA-regulated entities' resilience against information security incidents (including cyber-attacks) and their ability to respond swiftly and effectively in the event of a breach.

Compliance is not just an IT problem. It requires a rapid, whole of organisation strategy. The board, senior management, audit and operational functions are all directly impacted by this standard and in some cases, liable.

There are practical ways to understand your readiness and degree of compliance right now. While a deadline is looming, there is plenty that can be done to ensure you meet the standard by contacting FirmGuard now.

Key Objective

To minimise 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).

What is Prudential Standard CPS 234?

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 that is appropriate for the organisation and its risks.

The Board of an APRA-regulated entity is ultimately responsible for ensuring that the entity maintains its information security.[1]

[1] Prudential Standard CPS 234 Information Security information paper for Public Release, APRA 2019.

How to comply with Prudential Standard CPS 234

The centrepiece of CPS 234 is the requirement on APRA-regulated entities to implement a framework which classifies information assets by:

Criticality
The potential impact of a loss of availability

Sensitivity
The potential impact of a loss of confidentiality or integrity

This is essentially a risk assessment of the effects that a loss of availability or integrity of the information assets would have on the entity. The Board of an APRA-regulated entity is then responsible for ensuring that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets.

Discuss your requirements and concerns to explore how we can help, call **1300 FIRMGUARD** (1300 347 648) or email us at **enquiries@firmguard.io**

firmguard.io

FirmGuard
SECURITY ANALYTICS

Key Requirements

Roles and responsibilities
From July 1, 2019, the board will be accountable for information security and cyber incidents.

Information security capability
Your security capability must be appropriate for your organisation and its risks.

Classification of all information assets
All information assets must be classified by criticality and sensitivity including those managed by third parties.

Internal audit
Subject matter experts must conduct information security specific assurance.

Controls testing
Testing of information security controls must be appropriate, structured, orderly, comprehensive, and conducted by specialists.

APRA notifications
You are required to notify APRA of information security incidents and in some circumstances, security control weaknesses.

Who is FirmGuard Security Analytics?

FirmGuard is a dedicated team of information security consultants that provide risk assessments, gap analysis, remediation strategies and services, security improvement planning and an ongoing managed service to maintain your compliance and cybersecurity strategy.

We call ourselves FirmGuardians.

Our information risk experts execute appropriate assessment activity in developing an organisation's risk management strategies and preparing it for changes in both the current threat landscape, and the regulatory environment.

FirmGuard was founded by a team of IT and Information Security professionals with decades of experience behind them, to create a "safe pair of hands" for our clients and help them navigate the complexities of cybersecurity threats to your business and livelihoods.

We bridge the communication gap between the technical experts and business leaders, Board members and Directors accountable for managing cybersecurity.

Steps toward Compliance

Assess your readiness to comply with APRA's Prudential Standard CPS234

1. GAP Assessment
2. Extension application (if required)
3. Remediation
4. Compliance
5. Ongoing Management and Compliance
6. Periodic and Tailored Reporting to Executive and Board

Contact us on 1300 FIRMGUARD or enquiries@firmguard.io to **Assess your Readiness to Comply**