FORTRA

FACT SHEET (Boldon James)

Achieving Compliance with APRA Prudential Standard CPS 234

Protecting the Sensitive Data of Australian Citizens

With the financial sector under ever-increasing cyber-attack, the Australian Prudential Regulation Authority (APRA) has released the Prudential Standard CPS 234 in response. This ensures that APRA-regulated entities have established sufficient protections to guarantee information security.

Regulated entities – which include banks, neobanks, credit unions, insurers, superannuation funds, private health insurance companies, and non-operating holding companies – must now demonstrate compliance with the standard rather than just following the guidance. The responsibility for this lies with the board of an APRA-regulated entity.

Organisations must demonstrate the maintenance of an information security capability that aligns with the vulnerabilities and threats to which their information assets are exposed and enables the continued operation of the entities. APRA CPS 234 strongly focuses on identifying and managing information assets – i.e. corporate data.

There is no need for any organisation to wait - determining the risks to be managed, understanding what data needs to be protected, starting to secure it, and putting resources and policies in place. The best place to start is always with data classification.

The cost of non-compliance with APRA CPS 234 is measured in terms of reputation loss and damage to the brand – no organisation wants to be known for not taking appropriate care of private and personal information. Additionally, the regular data protection audits recommended in the regulation make it more likely that incidences of non-compliance will get noticed.

Key CPS 234 Requirements

- Clearly define the information security-related roles and responsibilities of the board, senior management, governing bodies and individuals.
- Implement and maintain information security controls that are proportional to the threat posed against your information assets and enable the entity's continued sound operation.
- Implement controls to protect information assets in line with the criticality and sensitivity of those assets and undertake regular testing regarding their effectiveness.
- Notify the APRA about material information security incidents.

The First Steps When Securing Your Sensitive Data

The first step in using a data classification approach to ensure compliance is understanding all the personal or sensitive data you hold and the potential risks to its security.

You will need to ask:

- What data do you already hold?
- What data is being collected, and from where?
- Where is it being stored and processed?
- Why do you have it?
- How sensitive is it?
- How is it accessed, used or shared, internally or externally?

The data should then be classified or tagged according to its sensitivity. Once you have singled out the most confidential information, you can determine what higher-grade controls should be applied to ensure it is sufficiently protected.

Data Classification and a Culture of Compliance

The sheer volume of unstructured data in financial firms, combined with hackers' growing professionalism and technical abilities to breach perimeters, make it impossible to rely on people and processes alone to manage sensitive personal data appropriately.

Data classification embeds a culture of compliance in an organisation, involving users in identifying, managing and controlling regulated data while automating parts of the protection process to enforce rules and policies consistently.

Classifying data as a first step in addressing CPS 234 will enable the protection strategy and solutions you implement to be built around the types of data you have, and the levels of security they require.

Visit boldonjames.com for more information on how data classification can protect your sensitive data and help create a culture of compliance.

How Can Boldon James Help?

Market leading data classification from Boldon James supports compliance with the APRA Prudential Standard CPS 234 :

- is used in large financial firms with a wide variety of data classification policies.
- supports a strong, scalable and granular approach to data classification.
- can manage complex classification requirements that persist for the entire document lifecycle.
- its persistent metadata protects all emails, documents and other unstructured data from unintended data loss via email and other exits This metadata also improves the flow of information assets to third parties.
- metadata labels drive additional security controls and solutions, such as DLP, encryption and rights management
- provides ease of management for the organisation plus strong user support through extensive education and alerting.
- provides a strong audit trail for classified data by providing critical audit information on classification events to enable remediation activity and demonstrates a compliance position to regulatory authorities.
- orchestrates data management solutions, such as data retention and archiving, to ensure adherence to data storage requirements

CPS 234 encourages good security practices within financial institutions and has put the main responsibility and accountability onto the board. In the face of such a varied attack landscape, in a sector where digital platforms are now the norm, this is to be welcomed.

But compliance with CPS 234 can be a challenge. That's why the right data classification tool can be your organisation's most effective tool for CPS 234 compliance.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

