CPS 234.

Are you ready?

Red Piranha

CPS 234. Launched on 1 July 2019. Deadline where assets are managed by third-party service providers, 1 July 2020; less than three months away. Feeling the pressure yet?

For those unaware of what CPS 234 is, let us recap. The Australian Prudential Regulation Authority, or APRA for short, is an independent statutory authority that supervises institutions across banking, insurance and superannuation, promoting financial system stability in Australia. APRA, a vital regulator of the financial services industry, also happens to be the sole government body overlooking the holdings of Australian assets worth $6.5 trillion. Given the realistic nature of evolving threat environments, CPS 234 mandates regulated entities identify the security threats that loom over it and related third parties.

Formerly Prudential Practice Guide (PPG) 234, CPS 234, or known in full as Consolidating Prudential Standard 234, relates explicitly to Information Security within these sectors. This Prudential Standard aims to ensure that an APRA regulated entity takes measures to be resilient against information security incidents (including cyberattacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats. A key objective of this standard is 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.

ISO
27001:2013
Australian Government
Australian Signals Directorate
PCI
APRA
Australian Prudential Regulation Authority
GDPR
NIST
CIS

Defined within the standard is to whom this standard applies. In short, this Prudential Standard applies to all "APRA regulated entities". An APRA regulated entity is either a financial institution authorised under the Banking Act, an insurer governed by the Insurance Act or the Life Insurance Act, a private health insurer registered under the PHIPS Act, or a Register of Superannuation Institutions (RSE) licensee regulated under the SIS Act in respect of their business operations.

If you are familiar with the ISO 27001 Information Security Management System (ISMS) international standard, reading CPS 234 would feel like deja vu. You will not be wrong in that feeling either. Per mappings between the requirements of CPS 234 and the Clauses and relative Annexes and Controls of ISO27001:2013, when performing compliance reviews or audits, information security experts will consider information gathered per numerous ISO 27001:2013 Clauses and their respective Annexes and Controls including, but in no way limited to,

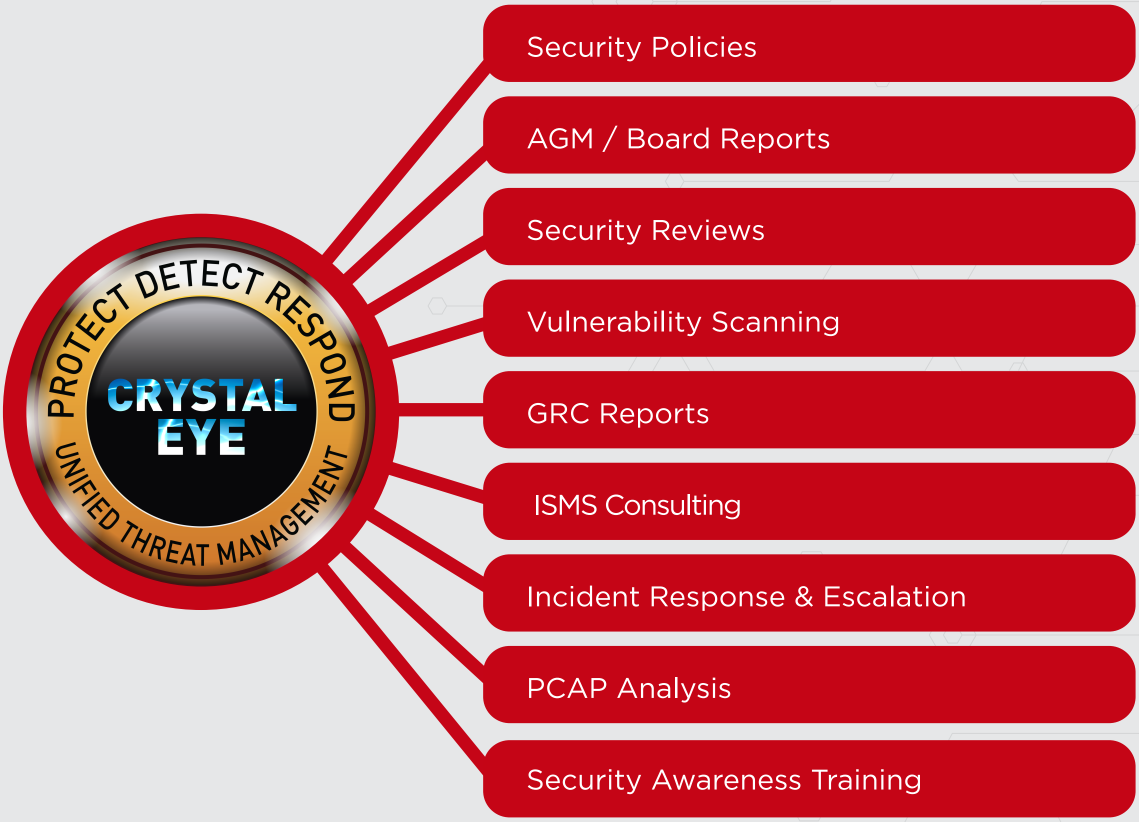
- Clause 4.4 – Information Security Management System
- Clause 5.1 – Leadership & Commitment
- Clause 5.2 – Policy
- Clause 5.3 – Organisational Roles, Responsibilities, and Authorities
- Clause 6.1 – Actions to Address Risks and Opportunities
- Clause 6.2 – Information Security Objectives and Planning to Achieve them
- Clause 7.1 – Resources
- Clause 7.2 – Competence
- Clause 8.1 – Operational Planning and Control
- Clause 8.2 – Information Security Risk Assessment

- Clause 8.3 – Information Security Risk Treatment
- Clause 9.1 – Monitoring, Measurement, Analysis and Evaluation
- Clause 9.2 – Internal Audit
- Clause 9.3 – Management Review
- Clause 10.1 – Non-Conformity and Corrective Action
- Clause 10.2 – Continual Improvement

There is significant overlap for those that are ISO 27001 certified with CPS 234; however, there are some critical differences that organisations must understand. We will touch on these a little later.

When it comes to CPS 234, the Board (or Board of Directors for an RSE, or the senior officer outside of Australia for a foreign ADI) of an APRA-regulated entity is ultimately responsible for the information security of the regulated entity. CPS 234 explicitly states that "The Board of an APRA-regulated entity is ultimately responsible for Information Security." The Board must ensure that it maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity. APRA regulated entities must also clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions. In ISO 27001, this is control A.6.1.1 where Information Security Roles and Responsibilities are defined.

Notwithstanding these definitions, APRA regulated entities must maintain an information security capability, an information security policy framework, asset identification and classification, incident management, implementation and effectiveness testing of controls, audits, and more. For many of these regulated entities, these requirements now add onto other compliance obligations further levying extra responsibility, increasing the risk of a higher level of cybersecurity fatigue. But before jumping into the deep end and stressing over CPS 234 compliance, it helps to take a step back and look at the broader information security requirements and strategy of the organisation.



Firstly, APRA has several standards and guidelines related to information security. CPS 234 activities need consideration alongside APRA's other requirements such as CPS 220 - Risk Management, CPS 231 - Outsourcing, or CPG 235 - Managing Data Risk. One aspect of CPS 234 to also take note of, is that it does not define any "controls" that require implementation; it merely tells you what the expectations are and leaves the rest up to you. Let us take, for example, a financial services organisation that processes credit card data and requires compliance against CPS 234. As they process credit card data, they will have obligations to comply with the Payment Card Industry Data Security Standard (PCI DSS). This organisation also wants to become ISO 27001 certified, being the international ISMS standard. In tackling ISO 27001 and PCI DSS, this organisation will comply with CPS 234. So as a summary, ensure you consider your broader information security requirements and strategies which may overlap with CPS 234. These could include the Privacy Act, including the Notifiable Data Breaches amendment, SOC 2, PCI DSS, ISO 27001, EU GDPR, NIST Cyber Security Framework, or even the Australian Information Security Manual (ISM) if you are working with Federal Government.

To those critical differences stated earlier, it is imperative to note that where a third party manages information assets, 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. For the avoidance of doubt, this applies to ALL information assets managed by related parties and third parties, not only those captured under agreements with service providers of outsourced material business activities under CPS 231 Outsourcing or SPS 231 Outsourcing. Another critical difference to take note of is that CPS 234 followed the footsteps of the European Union (EU) 's General Data Protection Regulation (GDPR) when it comes to incident notifications. Receiving royal assent and enforced from 22 February 2018 was the Notifiable Data Breaches amendment to the Australian Privacy Act. This amendment gives organisations thirty (30) days to complete assessments and notify the Office of the Australian Information Commissioner of a potential data breach. The EU GDPR and accordingly CPS 234 explicitly states that 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. Additionally, regulated entities must notify APRA as soon as possible and, in any case, no later than ten (10) business days, after becoming aware of a material information security control weakness that it expects will not be promptly remediated.

Ongoing changes in regulations and the ever-growing number of cybersecurity threats and attack vectors call for entities to further enhance their policies and use innovative methods to comply not only with CPS 234 but also with other compliance obligations. Adoption of a mixture of automated and manual compliance solutions require consideration by these regulated entities. Organisations looking to meet their compliance obligations should look no further than Red Piranha Limited's ISO27001:2013 Certified Crystal Eye Unified Threat Management (UTM) Platform and Red Piranha Limited's Governance, Risk and Compliance (GRC) Consultancy Services, including its Virtual Chief Information Security Officer (vCISO) services.

Businesses of all types are under increasing pressure to meet a range of compliance requirements such as ISO 27001, CPS 234, ISM, PSPF, GDPR, HIPAA or PCI to demonstrate maturity with information and cybersecurity. Chief Information Security Officers (CISO's) are becoming sought after, and with that demand comes increasing cost; often unattainable for typical small to medium-sized entities. Having all the skills and knowledge without the liability and expense of an additional employee is only one of the many benefits of hiring a vCISO.

According to the Annual Cisco 2019 Asia Pacific Chief Information Security Officer (CISO) Benchmark Study 1, which compares 11 countries and their cybersecurity standing, interviewing almost 2,000 security professionals, 209 of which were Australian CISOs,

- 84% of organisations in Australiasuffered a breach that cost them over $1 million, which is higher than any other country, in the APJC region and globally
- 69% of Australian organisations reportedreceiving more than 100,000 alerts every single day, which ismore than double 2018's figureof 33%
- 75 percent of Australian organisationsexperienced an outage of 5 -16 hourswhich islonger than the global averageof 43 percent
- Australian businesses are experiencingdouble the level of Cybersecurity Fatiguein comparison to the worldwide average, with Australia at 65% compared to the global average of 30%

Commenting on the findings of the study, Cisco Australia and New Zealand's Director of Cybersecurity, Steve Moros, says,

"Businesses are now facing challenges from all sides – it is a constant battle. Our report shows that data breaches and attacks are increasingly costing businesses and they are having to fight constant levels of attacks and in turn suffer cyber fatigue where they don't have the resources both in people and time to proactively protect their business."

Now that you know the basics of CPS 234, are you ready to become and remain compliant? With certified experts and auditors across all the standards and frameworks listed above amongst others on staff, Red Piranha, an Australian owned and operated cybersecurity firm, and manufacturer of the ISO 27001 Certified Crystal Eye Unified Threat Management (UTM) Platform, is your trusted advisor. Let our experts take some of that pressure off you and run hand in hand with you and your teams to achieve compliance. For more information or to get started, contact one of our business development managers today!