eBook

APRA Level Security Compliance

What you need to know about CPS 234

ipsi®

simplifying payments

Introduction

On 1st July 2019, the Australian Prudential Standards Authority (APRA) will enforce a new prudential standard (CPS 234) to address information and cybersecurity for APRA regulated entities.

APRA's new standard underlines and reinforces the need for APRA regulated entities to increase their focus on IT security. Growth in the use of cloud technology and increased reliance on IT assets, including software and hardware for data collection and transmission have heightened the expectations of both stakeholders and customers for improved IT security risk management.

The main objective of the release of CPS 234 is to reduce the likelihood and impact of information security incidents on the confidentiality, integrity or availability of information assets, including information assets managed by related or third parties.

CPS 234 identifies that the ultimate responsibility for information security lies with the **Board of the APRA-regulated entity.** IPSI contends that most companies don't appreciate the size and extent of the threats to their information assets and often lack the understanding and tools necessary to estimate the financial exposure.

Can you afford the risk?

$1.99 million
Average total cost of a data breach

$108 per card
Average cost per stolen record

Source: 2018 Cost of Data Breach Study - Ponemon Institute - Australian Data

The Board must also clearly define the roles and responsibilities for information security management including the roles of the Board, senior management, governing bodies and individuals within the organisation to comply with CPS 234.

The new standard also recognises that information security management is an on-going process. Therefore, the standard requires that controls are implemented to protect information assets and that these controls are systematically tested to ensure their effectiveness and that APRA is notified of any material information security incidents.

19,442 records

is the average number of breached records for Australian organisations in 2018

Source: 2018 Cost of Data Breach Study - Ponemon Institute

How can IPSI help?

The APRA security requirements are far-reaching, IPSI can assist APRA regulated entities to align with the standards in the following ways:

Data Scanning Technology

By leveraging IPSI's advanced scanning service, organisations can scan their environment to identify sensitive customer data (PII & credit card data), which isn't adequately secured.

Scanning technology can also be used to calculate financial exposure and ensure cost-effective resource allocation, based on a prioritised security methodology.

Periodic scanning and reporting also demonstrates active governance, responsibility and accountability across departments.

Data Security and the Elimination of On-Premise Data Storage

Recent cyber attacks within the Australian Insurance industry highlight that virus protection can't guarantee data protection. Securing the perimeter is critical but it doesn't eliminate the risks of on-premise storage of sensitive data. Best practise is replacing credit card data storage with non-financially sensitive tokens via advanced security certified cloud services, thereby reducing the risk associated with a data breach.

Next Generation Payment Systems

Securing and replacing legacy inhouse payment processes and traditional banking products with advanced e-commerce services can improve security while reducing the costs, risks and lead times associated with security compliance.

Ensuring all your third party service providers which store, process, or transmit customer credit card data are independently certified as Level 1 PCI DSS (Payment Card Industry Data Security Standard) compliant will further improve your companies security position.

IPSI can assist companies to become security compliant and/or it can replace legacy technology with secure yet highly flexible e-commerce capabilities across a range of channels, mobile, internet, call centre, SFTP, batch including data at rest.

Understanding IT Security Risk

When reviewing prudential standard CPS 234, it's important to understand how IT security risk is viewed in relation to APRA regulated entities.

For the standard, IT security risk is defined as the potential compromise of an information assets confidentiality, integrity and availability. These are defined as:

Confidentiality: Only authorised access is permitted.

Integrity: Completeness, accuracy and freedom from unauthorised change.

Availability: Accessibility and useability when required.

Any compromise of the confidentiality, integrity or availability of information assets can have a detrimental impact on the regulated entity, resulting in failure to meet its business objectives.

With this in mind, IT security risk is described as the risk of loss due to inadequate or failed internal processes, people and systems or from external events, resulting in a compromise of an IT asset's confidentiality, integrity or availability.

Ultimately, an APRA-regulated entity must have information security capability which corresponds with the size and threat to its information assets and enables the continued sound operation of the entity.

> "A significant information security breach at an APRA-regulated entity is almost certainly a question of when – not if. In a worst-case scenario, a major breach could even force a company out of business. As a result, APRA is fast-tracking implementation of this standard, and expects all regulated entities to meet its requirements by 1 July"
>
> **Geoff Summerhayes**
> **APRA Executive Board Member**

How can IPSI help?

Outsourcing credit card security compliance to a specialist service provider such as IPSI reduces the financial and resource burden associated with securing credit card data. IPSI offers the added benefit of strategic bank independence, advanced digital capabilities and and improved customer experience.

Responsibility of the Board

Under APRA's prudential standard CPS 234, the Board of a regulated entity is ultimately responsible for information security.

2018 was a year of significant change in the world of information security compliance.

In February 2018, Australia's Notifiable Data Breach Scheme legislation became law, and on the 25th May, Europe's General Data Protection Regulations (GDPR) came into effect and unified all current laws related to information protection across Europe.

The rise in the size, scale and cost of data breaches underlines the need for Boards to bear the ultimate responsibility for information security. Within CPS 234, APRA recommends that boards consider the following:

☑ Roles and Responsibilities
☑ Information Security Capability
☑ Policy Framework
☑ Implementation of controls
☑ Testing Control Effectiveness
☑ Internal Audit

> "There is a clear link between PCI DSS compliance and an organisations ability to defend itself against cyber attacks"
>
> **Rodolphe Simonetti**
> **Global Managing Director**
> **Verizon**

This new standard sits alongside their updated guidance around the use of cloud computing services as APRA regulated entities are increasing their use of cloud-based platforms to manage information assets as well as enable digital innovation (such as payments technology), reduce operational costs and achieve greater operational efficiency.

Key Points

✓ The Board is ultimately responsible for the information security of the entity.

✓ The Board must ensure the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets.

✓ Many companies underestimate the risks and the costs associated with data security and compliance. Due to staff exposure to more inflexible service capabilities, they sometimes overestimate the complexity and lead times associated with upgrading legacy inhouse payment or banking payment processes.

Roles & Responsibilities

While the Board is ultimately responsible for information security, APRA doesn’t impose restrictions on how roles and responsibilities are delegated to individuals under CPS 234.

Definitions of roles and responsibilities are commonly achieved in a variety of ways. They may include but are not limited to; role statements, policy statements, reporting lines and charters of governing bodies.

The entity must identify security-related roles and responsibilities of the Board, senior management, governing bodies and individuals responsible for decision-making, approval, oversight, operations and other information security functions. These may typically be:

☑ Information security steering/oversight committee;
☑ Risk management committee (Board and management levels);
☑ Board audit committee;
☑ Executive management/executive management committee;
☑ Chief information officer (CIO)/IT Manager;
☑ Chief information security officer (CISO)/ IT security manager;
☑ Information security operations/ administration; and
☑ Management (business and IT)

APRA recognises that roles and responsibilities that relate to information security can exist across different business areas and/or functions, including third parties. Entities must ensure that any issues relating to accountability or lack of ownership due to this fragmentation are addressed through effective compensating measures such as establishing a virtual security group including members with information security roles and responsibilities.

77.8%

of Asian-Pacific companies

fail to maintain all PCI DSS controls 12 months after achieving 100% compliance.

Source: Verizon 2018 Payment Security Report

Key Points

- ✓ Information security roles and responsibilities must be clearly defined.
- ✓ Boards, governing bodies and individuals must define their information requirements and define escalation paths to effectively discharge their roles and responsibilities.
- ✓ IPSI believes that a PCI DSS Compliance role and/or governance group should be established to ensure that customer credit card data security compliance is maintained.
- ✓ Service providers which store, process or transmit credit card data should be Level 1 PCI DSS certified and provide a responsibility matrix to ensure the roles and responsibilities of all parties are clearly defined.

Information Security Capability

An APRA-regulated entity must have information security capability which corresponds with the size and threats to its information assets and enables the continued sound operation of the entity.

Fundamental to effective information security capability is ensuring that the resources and the investment put in place to protect information assets are adequate.

These resources may include investing in more specific information security capabilities such as new infrastructure, third-party expertise, on-going security testing, threat intelligence and incident response capability. Other capabilities, as identified by APRA include:

☑ Vulnerability and threat management, including situational awareness and intelligence;
☑ Information security operations and administration;
☑ Secure design, architecture and consultation;
☑ Security testing, including penetration testing;
☑ Information security reporting and analytics;
☑ Incident detection and response, including recovery, notification and communication;
☑ Information security investigation, including preservation of evidence and forensic analysis; and
☑ Information security assurance.

APRA recommends that entities should have a forward-looking approach and actively maintain their information security capability, including on-going investment in resources, skills and controls.

How can IPSI help?

✓ **Data Scanning** - Find and secure sensitive data before the criminals do.

✓ **Secure Data Storage** - Eliminate on-site storage of sensitive data and replace it with non-financially sensitive surrogate values (tokens) and leverage tokenisation and advanced cloud storage.

✓ **Credit Card Security** - Reduce or eliminate staff access to credit card data.

✓ **End-to-End Payment Security** - Introduce more secure end-to-end payment processes.

✓ **Ascertain Financial Exposure** - IPSI's scanning service can provide you with a clearer picture or your key financial asset exposure. Numbers and locations enabling estimation of your financial risks.

Policy Framework

An information security policy framework must be maintained and provide direction on responsible parties who have an obligation to maintain information security.

The typical structure of an information security policy framework would be to identify higher-level policies that are supported by underlying standards, guidelines and procedures. This policy framework would be guided by a set of information security principles that guide decision making. The policy framework would address the following areas according to APRA:

☑ Identification, authorisation and granting of access to information assets;

☑ Life-cycle management that addresses the various stages of an information asset's life to ensure information security requirements are considered at each stage, from planning and acquisition through to decommissioning and destruction;

☑ Management of information security technology solutions that include firewall, anti-malicious software, intrusion detection/prevention, cryptographic systems and monitoring/log analysis tools;

☑ Definition of an overarching information security architecture that outlines the approach for designing the IT environment (encompassing all information assets) from a security perspective (e.g. network zones/segments, endpoint controls, gateway design, authentication, identity management, interface controls, software engineering and location of information security technology solutions and controls)

☑ Monitoring and incident management to address the identification and classification of incidents, reporting and escalation guidelines, preservation of evidence and the investigation process;

☑ Expectations concerning the maintenance of information security when using third parties and related parties;

☑ Acceptable usage of information assets that define the information security responsibilities of end-users including staff, third parties, related parties and customers;

☑ Recruitment and vetting of staff and contractors;

☑ Information security roles and responsibilities;

☑ Physical and environmental controls; and

☑ Mechanisms to assess compliance with and the ongoing effectiveness of the informatrion security policy framework.

Customer credit card data should be treated with the utmost sensitivity. All third-party service providers that store, process, or transmit your customer credit card data should be independently assessed as level 1 PCI DSS certified.

The effectiveness and completeness of the policy framework should be evaluated periodically through a review of incidents and compared to other industry standards. Any change to an entities information assets or business environment should typically trigger a review of the policy framework.

Key Points

✓ The entity must maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats.

✓ The information security policy framework must provide direction on the responsibilities of all parties who have an obligation to maintain information security.

✓ Descoping credit card security compliance via cloud-based outsourcing with a Level 1 PCI DSS certified service provider would further reduce a companies security burden while aligning with the APRA security principals.

The true cost of non-compliance:

Ensuring compliance with the growing number of government and industry regulations such as CPS 234 can be a drain on already stretched resources. But research by the Ponemon Institute shows that non-compliance costs 2.71 times the cost of meeting compliance obligations.

The following statistics highlight the cost of compliance and non-compliance:

Cost of non-compliance vs compliance
“the annual cost of non-compliance runs at an average of $14.8 million compared to $5.5 million for compliance”

Cost of compliance by industry
“The cost of compliance varies significantly by the organisation’s industry sector, ranging from $7.7 million for media to more than $30.9 million for financial services.

Compliance expense categories
“companies spend most in compliance related technologies ($1.34 m) and incident response ($1 m)”

Compliance cost centres
“Data security is the highest cost centre for compliance with the average cost of data security $2 million dollars.

Source: The True Cost of Compliance with Data Protection Regulations Report 2017 - Ponemon Institute

IPSI Security Insight

IPSI has found that most companies store excess amounts of redundant customer credit data without appreciating the financial exposure associated with such storage.

Companies should review their information assets (especially credit card data), eliminate and reduce storage to a needs basis, then replace the data with non financially sensitive tokens via secure/pre certified cloud storage to further reduce security exposure and the security burden associated with the residual assets.

Asset Identification & Classification

Information assets must be classified based on criticality and sensitivity. These classifications must reflect the potential impact of an information security incident on the entity and the interests of depositors, policyholders, beneficiaries and customers.

Under CPS 234, **criticality** refers to the potential impact of a loss of availability and **sensitivity** means the potential impact of a loss of confidentiality and integrity.

Information assets include infrastructure, ancillary systems such as environment and physical access control systems and any information assets managed by third parties.

The challenge for APRA regulated entities is to develop a consistent methodology to classify information assets. CPS 234 recommends that entities develop a classification methodology to determine what an information asset is and the method for rating criticality and sensitivity.

The recording of information assets can also differ between entities. APRA recognises that some entities treat all information assets as independent for the purposes of classification, and some aggregate a combination of assets together (such as databases, operating systems and applications) and classify them as one information asset.

Under CPS 234, if an entity chooses to aggregate information assets together, then all of the individual components of the asset must inherit the highest criticality and sensitivity ratings of the constituent components.

Key Points

✓ All information assets must be classified based on criticality and sensitivity.

✓ A consistent methodology must be used and recorded to classify all information assets.

✓ Credit card data in terms of criticality and sensitivity should be treated with the upmost importance. Average cost per stolen credit card is $108 per card stolen.

Implementation of controls

Controls must be in place to protect information assets at all stages of their life-cycle, including those managed by a related or third party.

Critical to ensuring that controls remain effective at all stages of the information assets life-cycle is the allocation of responsibility and accountability to an information asset owner. CPS 234 recommends that the owner is an individual located within the business function that is most reliant on the information asset.

In the first phase of the information assets life-cycle, planning and design controls should be in place to ensure information security is incorporated within the information asset. The addition of new information assets should also have no impact on the information security of established assets which are maintained through on-going support and maintenance controls. APRA provides examples of categories of control, which include:

☑ Change Management - information security is addressed as part of the change management process, and the information asset inventory is updated;

☑ Configuration management —the configuration of information assets minimises vulnerabilities and is defined, assessed, registered, maintained, including when new vulnerabilities and threats are discovered and applied consistently;

☑ Deployment and environment management —development, test and production environments are appropriately segregated and enforce segregation of duties;

☑ Access management controls —only authorised users of software and hardware can access information assets (refer to Attachment B for further guidance);

☑ Hardware and software asset controls —appropriate authorisation to prevent security compromises from unauthorised hardware and software assets;

☑ Network design — to ensure authorised network traffic flows and to reduce the impact of security compromises;

☑ Vulnerability management controls — which identify and address information security vulnerabilities in a timely manner;

☑ Patch management controls — to manage the assessment and application of patches and other updates that address known vulnerabilities in a timely manner;

☑ Service level management mechanisms — to monitor, manage and align information security with business objectives;

☑ Monitoring controls — for timely detection of compromises to information security;

☑ Response controls — to manage information security incidents and feedback mechanisms to address control deficiencies;

☑ Capacity and performance management controls — to ensure that availability is not compromised by current or projected business volumes; and

☑ Service provider management controls — to ensure that a regulated entity's information security requirements are met.

While this list of controls is comprehensive, APRA recommends that entities regularly assess the completeness of their controls by reviewing industry practices.

Information assets managed by third and related parties.

CPS 234 recognises that many information assets are managed by third-parties. In this situation, regulated entities must evaluate the service suitability and security and understand how security is maintained to secure the information assets.

Too often businesses are using third party service providers to store, process or transmit customer card data who are not level 1 PCI DSS certified, in the mistaken belief that they do not need to be as they are not the "credit card merchant".

IPSI has been independently certified as meeting the highest levels of credit card security available (Level 1 PCI DSS certified).

Incident management

An APRA-regulated entity must have robust mechanisms in place to detect and respond to actual and potential information security incidents in a timely manner.

Response plans to information security incidents must be maintained by APRA regulated entities. Such incidents may include:

☑ Malware infection (e.g. virus, ransomware);
☑ Data breach (customer or internal data);
☑ Compromise of staff or customer credentials (e.g. as the result of a phishing attack);
☑ Denial-of-service attack;
☑ Hack of an internet-facing platform;
☑ Website defacement; and
☑ Compromise by an advanced persistent threat.

The response plan must include mechanisms to manage all stages of response from detection to post-incident review as well as reporting and escalation of incidents to the board, governing bodies and individual who are responsible and accountable for information assets.

To ensure response plans are up-to-date, entities must review and test its information security response plans to ensure they remain effective and fit for purpose.

Key Points

✓ Mechanisms must be in place to detect and respond to incidents in a timely manner.

✓ Response plans must be reviewed annually to ensure they are effective and fit-for-purpose.

Testing control effectiveness & audits

An APRA-regulated entity must test and audit the effectiveness of its information security controls through a systematic testing program by skilled and functionally independent specialists.

Systematic testing is critical to ensure security controls are effective and must be conducted annually under CPS 234. The nature and frequency of the testing must be commensurate with:

☑ the rate at which the vulnerabilities and threats change;
☑ the criticality and sensitivity of the information asset;
☑ the consequences of an information security incident;
☑ the risks associated with exposure to environments where the APRA regulated entity is unable to enforce its information security policies; and
☑ the materiality and frequency of change to information assets.

In situations where a third or related parties manage information assets, the entity must assess whether the information control testing of the third party is adequate and has been independently certified as meeting the relevant security standards.

Any test results that identify potential vulnerabilities must be escalated and reported to the board and senior management.

Internal Audit requirements

To support the systematic testing program, regulated entity's internal audit activities must include a review of the design and operating effectiveness of information security controls, including those maintained by related parties and third parties. The entity must ensure that security control assurance is provided by personnel suitably qualified to provide such assurance.

Key Points

✓ A systematic testing program must be in place to test the effectiveness of information security controls.

✓ Audit activities must include a review of the design and operating effectiveness of information security controls.

APRA Notification

In the event of an information security incident, entities must notify APRA as soon as possible and no later than 72 hours after they become aware of the incident.

The information to be provided to APRA should include:

☑ name of the APRA-regulated entity;
☑ date and time/period of the incident;
☑ date and time when the incident was assessed as material;
☑ incident type;
☑ incident description;
☑ current status of incident; and
☑ mitigation actions are taken or planned (where available).

Regulated entities are also required to notify APRA, no later than 10 business days after it becomes aware of a material information security control weakness which the entity expects it will no be able to remediate in a timely manner. In this situation, the entity is expected to provide APRA with the following information:

☑ name fo the APRA-regulated entity;
☑ date and time when the control weakness was assessed as material;
☑ control weakness description;
☑ current status of control weakness; and
☑ mitigation actions taken or planned.

Identifying control weaknesses should be achieved in several ways including control testing, assurance activities, vulnerability notification and through timely notification by third and related parties.

Key Points

✓ APRA must be notified within 72 hours of an information security incident.

✓ APRA must be notified no later than 10 business days after they become aware of a material information security control weakness.

Our Solutions

Enterprise Payment Solutions

Mobile, credit card, call centre, phone (IVR), tokens? Your customers expect simple, hassle-free payments. Our extensive selection of payment solutions gives you the flexibility to accept payments the way you want to in a highly secure and compliant manner.

PCI DSS Remediation

If you accept, process or transmit credit card payment data, then you and any of your third-party service providers must be PCI DSS compliant. Our PCI DSS expertise and payment solutions help you reduce the cost, risk and lead times associated with achieving and maintaining PCI DSS compliance.

Contact Centre Solutions

Our flexible, scalable and integrated contact centre solutions ensure that no credit card data enters your contact centre, simplifies the agent payment process and enhances the customer experience while reducing your exposure to fraud.

Data Discovery Platform

Sensitive data, such as credit card and PII (Personally Identifiable Information) are a gold mine for cyber criminals. Identifying and securing customer data is critically important to today's businesses. Our data discovery platform is a powerful software tool that will scan, locate and secure sensitive data across your IT environment.

To discuss how we can help you achieve security compliance, email us at assistance@ipsi.com.au or call 1300 975 630 today.

References

APRA Prudential Standard CPS 234 Information Security accessed June 2019 at https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf

Prudential Practice Guide, Draft CPG 234 Information Security accessed June 2019 at https://www.apra.gov.au/sites/default/files/draft_prudential_practice_guide_cpg_234_information_security_march_2019.pdf

2018 Cost of Data Breach Study - Ponemon Institute, July 2018

Cloud Computing in Insurance Report – Thematic Research, HTF Market Intelligence 31st August 2018

Verizon 2018 Payment Security Report accessed June 2019 at https://enterprise.verizon.com/resources/reports/2018_payment_security_report_en_xg.pdf

The True Cost of Compliance with Data Protection Regulations - Ponemon Institute December 2017 accessed July 2019 at http://dynamic.globalscape.com/files/Whitepaper-The-True-Cost-of-Compliance-with-Data-Protection-Regulations.pdf

About us

ipsi®

simplifying payments

The IPSI team have helped ASX top 50 and fortune 500 companies implement best-of-breed payment technology that bridges the gap between traditional payment products, and companies' unique requirements.

The rapid growth of digital commerce has meant that payment capability, PCI DSS compliance, cybersecurity and storage of sensitive data is a crucial consideration when assessing payment technology.

IPSI has been part of this growth, successfully providing highly flexible payment and data security solutions to enterprise level clients for over 10 years. The IPSI team has managed some of Australia's largest e-commerce and PCI DSS tokenisation projects in Australia. Services range from cloud-based payment processing, tokenisation services, contact centre payment solutions, flexible mobile and pay-by-phone (IVR) services, PII data scanning and storage to PCI DSS remediation solutions.

To discuss how we can help achieve security compliance, email us at assistance@ipsi.com.au or call 1300 975 630.

1300 975 630
www.ipsi.com.au

ipsi®

Jones Bay Wharf
6, 26-32 Pirrama Rd,
Pyrmont, Sydney NSW 2009 Australia