UNDERSTANDING APRA CPS REGULATIONS AND THEIR SIGNIFICANCE FOR REGULATED ENTITIES

This paper provides an overview of the Australian Prudential Regulation Authority (APRA) prudential standards known as CPS (Cross-Industry Prudential Standards) in relation to the Technology Risk Management domain. It explores the rationale behind these regulations, and their importance for APRA-regulated entities, and summarizes key points from CPS 232, CPS 234, CPS 231, and CPS 220.

APRA is responsible for regulating and supervising financial institutions in Australia to ensure their stability and protect the interests of depositors, policyholders, and the broader financial system. To achieve these objectives, APRA has established a set of prudential standards, known as CPS regulations, which cover various aspects of financial institutions' operations.

WHAT IS THE RATIONALE FOR THESE CPS REGULATIONS?

1. **Financial Stability:** CPS regulations are designed to enhance the stability of APRA-regulated entities, reducing the risk of financial crises, and safeguarding the interests of depositors and policyholders.
2. **Risk Management:** These regulations ensure that regulated entities have robust risk management frameworks in place, allowing them to identify, assess, and manage risks effectively.
3. **Consumer Protection:** CPS regulations aim to protect consumers by ensuring that financial institutions maintain adequate capital, manage their risks prudently, and comply with relevant laws and industry standards.

WHY ARE THEY IMPORTANT FOR APRA-REGULATED ENTITIES?

1. **Compliance:** Compliance with CPS regulations is mandatory for APRA-regulated entities. Non-compliance can lead to regulatory action, including fines and sanctions.
2. **Financial Stability:** Adherence to CPS regulations helps entities maintain financial stability, which is crucial for their long-term viability and reputation.
3. **Risk Mitigation:** These regulations provide a framework for identifying and managing risks effectively, reducing the likelihood of financial losses and reputational damage.

KEY APRA CPS REGULATIONS FOR TECHNOLOGY RISK MANAGEMENT:

CPS 220 - RISK MANAGEMENT

CPS 220 outlines requirements for risk management, including governance, risk identification, measurement, and mitigation. It also mandates stress testing and capital adequacy assessments.

CPS 231 - OUTSOURCING

This standard focuses on managing risks associated with outsourcing arrangements. It emphasizes due diligence when selecting service providers and ongoing monitoring of outsourced activities.

CPS 232 - BUSINESS CONTINUITY MANAGEMENT

This standard requires regulated entities to maintain comprehensive business continuity plans to ensure they can continue operations during disruptions. It emphasizes the importance of testing and reviewing these plans regularly. It will be replaced by CPS 230 in July 2025.

CPS 234 - INFORMATION SECURITY

CPS 234 mandates robust information security practices, including cybersecurity measures, to protect sensitive data. It requires entities to report breaches promptly and implement comprehensive incident response plans.

APRA CPS regulations play a critical role in maintaining financial stability, protecting consumers, and ensuring prudent risk management within APRA-regulated entities. Compliance with these regulations is not only a legal requirement but also essential for the long-term success and reputation of financial institutions in Australia. Understanding and adhering to these standards is paramount for all APRA-regulated entities.

CPS 230 - OPERATIONAL RISK

On the 1st of July 2025 CPS 230 will replace:

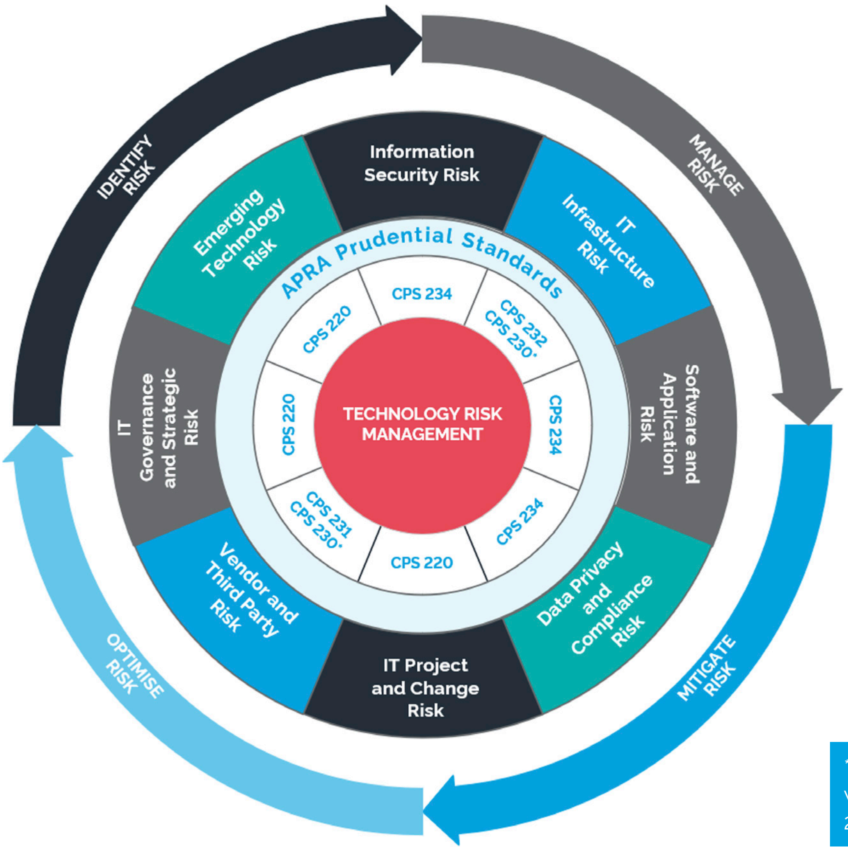
Prudential Standard CPS 231 Outsourcing (CPS 231), Prudential Standard SPS 231 Outsourcing (SPS 231), Prudential Standard HPS 231 Outsourcing (HPS 231), Prudential Standard CPS 232 Business Continuity Management (CPS 232) and Prudential Standard SPS 232 Business Continuity Management (SPS 232).

HOW WE CAN EMPOWER AND COLLABORATE WITH YOU

At PTS, we empower organizations, from the boardroom to the operations centres, to embrace uncertainty with confidence, instill resilience, and foster sustainable growth. Our approach hinges on a comprehensive understanding of the risk landscape, coupled with profound industry and regulatory knowledge. We collaborate with you on strategy, implementation, and capability building, addressing every facet of your journey towards success in the following areas:

We collaborate with our clients on strategy, implementation, and capability building – addressing every facet of their journey towards success.

PTS' TECHNOLOGY RISK MANAGEMENT MODEL


IDENTIFY RISK
MANAGE RISK
MITIGATE RISK
OPTIMISE RISK
Information Security Risk
IT Infrastructure Risk
Software and Application Risk
Data Privacy and Compliance Risk
IT Project and Change Risk
Vendor and Third Party Risk
IT Governance and Strategic Risk
Emerging Technology Risk
APRA Prudential Standards
CPS 234
CPS 232
CPS 230*
CPS 234
CPS 234
CPS 220
CPS 231
CPS 230*
CPS 220
CPS 220
TECHNOLOGY RISK MANAGEMENT

* CPS 231 and CPS 232 will be replaced by CPS 230 from 1 July 2025.

INFORMATION SECURITY RISK

Safeguarding critical data and systems against cyber threats and implementing robust cybersecurity measures.

IT INFRASTRUCTURE RISK

Ensuring resilience of IT systems against disruptions — plan for continuity and rapid recovery.

SOFTWARE AND APPLICATION RISK

Regularly assessing and managing application vulnerabilities to prevent breaches.

DATA PRIVACY AND COMPLIANCE RISK

Securing customer data, upholding privacy regulations and reporting breaches as required.

VENDOR AND 3RD PARTY RISK

Thoroughly assessing third-party services for security and compliance to protect data.

IT PROJECT AND CHANGE RISK

Planning IT projects with risk management in mind and ensuring changes are well-structured and aligned with strategy.

IT GOVERNANCE AND STRATEGIC RISK

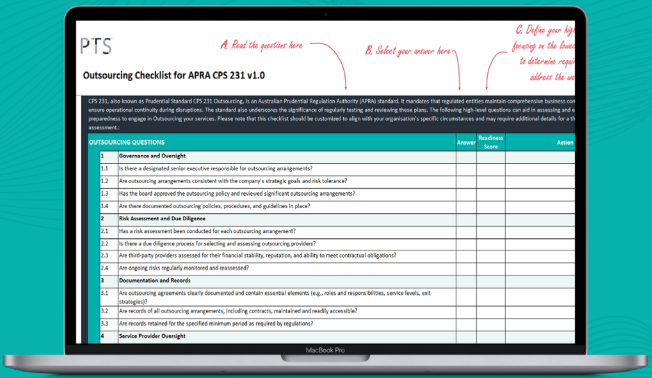
Integrating IT strategy into the overall governance framework, addressing potential strategic risks.

EMERGING TECHNOLOGY RISK

Understanding APRA's stance on emerging technologies and assess associated risks.

APRA CHECKLISTS

Are you responsible for or contributing towards the IT aspects of APRA compliance within your organisation? If so you may be interested in one or all of our free APRA checklists which can be accessed by either clicking on the buttons below or visiting https://pts.com.au/resources.



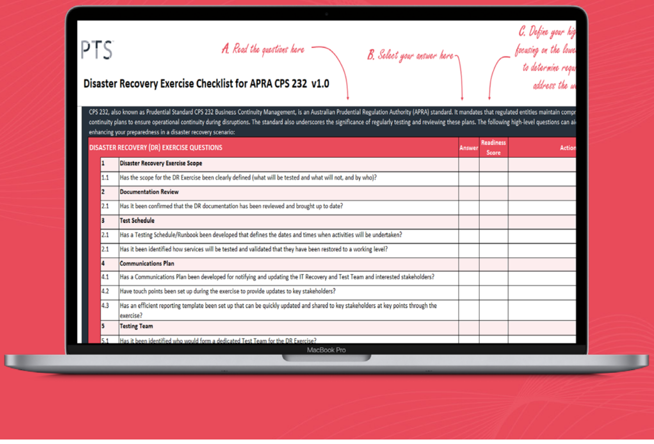
Outsourcing Checklist for APRA CPS 231 v1.0

CPS 231, also known as Prudential Standard CPS 231 Outsourcing, is an Australian Prudential Regulation Authority (APRA) standard. It mandates that regulated entities maintain comprehensive business con ensure operational continuity during disruptions. The standard also underscores the significance of regularly testing and reviewing these plans. The following high-level questions can aid in assessing and e preparedness to engage in Outsourcing your services. Please note that this checklist should be customized to align with your organisation's specific circumstances and may require additional details for a th assessment.:

OUTSOURCING QUESTIONS		Answer	Readiness Score	Action
1	**Governance and Oversight**			
1.1	Is there a designated senior executive responsible for outsourcing arrangements?			
1.2	Are outsourcing arrangements consistent with the company's strategic goals and risk tolerance?			
1.3	Has the board approved the outsourcing policy and reviewed significant outsourcing arrangements?			
1.4	Are there documented outsourcing policies, procedures, and guidelines in place?			
2	**Risk Assessment and Due Diligence**			
2.1	Has a risk assessment been conducted for each outsourcing arrangement?			
2.2	Is there a due diligence process for selecting and assessing outsourcing providers?			
2.3	Are third-party providers assessed for their financial stability, reputation, and ability to meet contractual obligations?			
2.4	Are ongoing risks regularly monitored and reassessed?			
3	**Documentation and Records**			
3.1	Are outsourcing agreements clearly documented and contain essential elements (e.g., roles and responsibilities, service levels, exit strategies)?			
3.2	Are records of all outsourcing arrangements, including contracts, maintained and readily accessible?			
3.3	Are records retained for the specified minimum period as required by regulations?			
4	**Service Provider Oversight**			

OUTSOURCING CHECKLIST FOR APRA CPS 231

Download Now



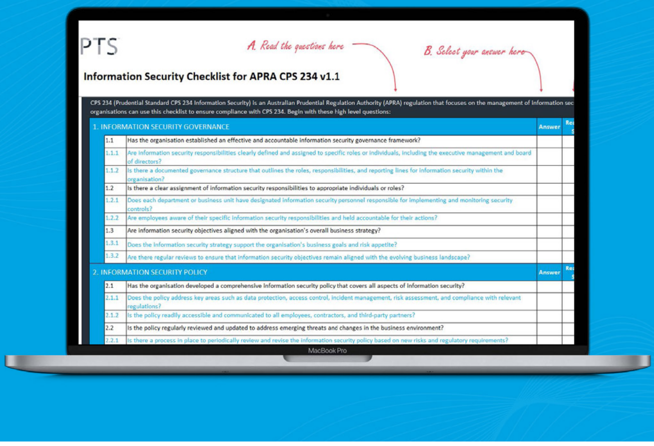
Disaster Recovery Exercise Checklist for APRA CPS 232 v1.0

CPS 232, also known as Prudential Standard CPS 232 Business Continuity Management, is an Australian Prudential Regulation Authority (APRA) standard. It mandates that regulated entities maintain compr continuity plans to ensure operational continuity during disruptions. The standard also underscores the significance of regularly testing and reviewing these plans. The following high-level questions can ai enhancing your preparedness in a disaster recovery scenario:

DISASTER RECOVERY (DR) EXERCISE QUESTIONS		Answer	Readiness Score	Actior
1	**Disaster Recovery Exercise Scope**			
1.1	Has the scope for the DR Exercise been clearly defined (what will be tested and what will not, and by who)?			
2	**Documentation Review**			
2.1	Has it been confirmed that the DR documentation has been reviewed and brought up to date?			
3	**Test Schedule**			
2.1	Has a Testing Schedule/Runbook been developed that defines the dates and times when activities will be undertaken?			
2.1	Has it been identified how services will be tested and validated that they have been restored to a working level?			
4	**Communications Plan**			
4.1	Has a Communications Plan been developed for notifying and updating the IT Recovery and Test Team and interested stakeholders?			
4.2	Have touch points been set up during the exercise to provide updates to key stakeholders?			
4.3	Has an efficient reporting template been set up that can be quickly updated and shared to key stakeholders at key points through the exercise?			
5	**Testing Team**			
5.1	Has it been identified who would form a dedicated Test Team for the DR Exercise?			

DISASTER RECOVERY EXERCISE CHECKLIST FOR APRA CPS 232

Download Now



Information Security Checklist for APRA CPS 234 v1.1

CPS 234 (Prudential Standard CPS 234 Information Security) is an Australian Prudential Regulation Authority (APRA) regulation that focuses on the management of information sec organisations can use this checklist to ensure compliance with CPS 234. Begin with these high level questions:

1. INFORMATION SECURITY GOVERNANCE		Answer	Re S
1.1	Has the organisation established an effective and accountable information security governance framework?		
1.1.1	Are information security responsibilities clearly defined and assigned to specific roles or individuals, including the executive management and board of directors?		
1.1.2	Is there a documented governance structure that outlines the roles, responsibilities, and reporting lines for information security within the organisation?		
1.2	Is there a clear assignment of information security responsibilities to appropriate individuals or roles?		
1.2.1	Does each department or business unit have designated information security personnel responsible for implementing and monitoring security controls?		
1.2.2	Are employees aware of their specific information security responsibilities and held accountable for their actions?		
1.3	Are information security objectives aligned with the organisation's overall business strategy?		
1.3.1	Does the information security strategy support the organisation's business goals and risk appetite?		
1.3.2	Are there regular reviews to ensure that information security objectives remain aligned with the evolving business landscape?		
2. INFORMATION SECURITY POLICY		**Answer**	**Re S**
2.1	Has the organisation developed a comprehensive information security policy that covers all aspects of information security?		
2.1.1	Does the policy address key areas such as data protection, access control, incident management, risk assessment, and compliance with relevant regulations?		
2.1.2	Is the policy readily accessible and communicated to all employees, contractors, and third-party partners?		
2.2	Is the policy regularly reviewed and updated to address emerging threats and changes in the business environment?		
2.2.1	Is there a process in place to periodically review and revise the information security policy based on new risks and regulatory requirements?		

INFORMATION SECURITY CHECKLIST FOR APRA CPS 234

Download Now