

Webinar: Demystifying CPS230

Your Guide to implementation of
Operational Resilience



Time

Approx. 30mins
with time for Q&A

Questions

write your question using the Q&A
area in the webinar and we'll answer
at the end.

Recording

Recording of this webinar will be
made available to all registered
participants

Agenda

- Overview and Key principles
- Key Considerations for implementation
- Demonstration of ReadiNow CPS230 Modules
- Q&A



Darren Jacobs
Chief Product Officer,
ReadiNow

CPS230 - Key Dates

July 2022	April 2023	July 2023	End 2024	1 July 2025	1 July 2026
APRA consults on draft CPS 230	APRA announces revised implementation timetable	APRA releases Final CPS 230*	Implementation <ul style="list-style-type: none">• Material service providers / critical operations identified*• Entities positioned to set tolerance levels set*	CPS 230 commences*	Transition ends for existing contracts with service providers

* Proactive transition period, regulated entities prepare for new requirements

CPS230 - Key Principles

Key Themes

Be prepared for risk events	Be resilient	Protect the entity and the community
--------------------------------	--------------	--

Areas of focus

- Critical operations
- Material service providers
- Business continuity
- Incident management
- Risk & Controls management

6 Key Areas of Action *to comply with CPS230*

- 1 Additional Board Reporting
- 2 Additional APRA Reporting Requirements
- 3 Amended Contractual Agreements with Service Providers
- 4 Enhance Operational Risk management
- 5 Enhance Business Continuity Planning
- 6 Enhance Management of Service Providers

1 Enhanced Board Reporting

The Board of an APRA-regulated entity is ultimately **accountable** for oversight of an entity's **operational risk management**. This includes **business continuity** and the management of **service provider arrangements**

1 Enhanced Board Reporting

Operational Risk



Operational Risk Profile & action items



Control testing results and remediation plans for any control gaps or deficiencies

Business Continuity



Report on any tolerance levels that are not met and the associated remediation plans



Audit Report on the credibility of BC plans to maintain critical operations

Service Provider Management



Report on Material Service Provider Compliance with Service Provider Management Policy

2 New APRA Notifications

The following notifications must be built into process'



Incidents that are likely to have material financial impact of the ability to maintain critical operations

72 Hours



After suffered a disruption to a critical operation outside tolerance

24 Hours



Entering into or materially changing an agreement with supplier that provides a service of a critical operation

20 Business Day



Prior to entering into an offshoring agreement with material service provider

Prior to entering into agreement



Register of Material Service Providers

Annually

4 Uplift Existing Process

Enhancements to:



**Operational Risk
management**



**Business Continuity
Planning**



**Management of Service
Providers**

CPS230 Implementation Checklist		
Clause	CPS230 Requirement	Completion of Action Items
Any principles		
11-30	effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
11-31	maintain its critical operations within tolerance levels through severe disruptions;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
11-32	manage the risks associated with the use of service providers;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12	must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external events and events;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must, to the extent practicable, prevent disruption to critical operations, adapt processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly after a disruption is over;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
14	must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Risk management framework		
15-30	governance arrangements for the oversight of operational risk;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-31	an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-32	internal controls that are designed and operating effectively for the management of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-33	appropriate monitoring, analysis and reporting of operational risks and resolution processes for operational incidents and events;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-34	business continuity plan(s) (BCP) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with senior but plausible scenarios;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-35	processes for the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	As part of the required review of the risk management framework under CPS 230 and SP1 330, an AFSA-regulated entity must review its operational risk management. The review must cover the aspects of operational risk management set out in paragraph 15;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	Operational risk management must be integrated into an AFSA-regulated entity's overall risk management framework and processes. Business continuity planning must be considered with, and not conflict or undermine, an AFSA-regulated entity's financial contingency planning;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
17	where AFSA considers an AFSA-regulated entity's operational risk management has material weaknesses, AFSA may require further information/action;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Role of the Board		
18	The Board of an AFSA-regulated entity is ultimately responsible for the oversight of an entity's operational risk management, including business continuity, and the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
19	The Board must ensure that the AFSA-regulated entity sets clear roles and responsibilities for senior management for operational risk management, including business continuity, and the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
20	The Board must (a) oversee operational risk management and the effectiveness of controls in maintaining the entity's risk profile within risk appetite with respect to operational risk;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness

Enhancements to:



Operational Risk management

Existing

- Para 26** ☐ Implementation of a process & systems by which operational risks identified, evaluated and assessed on a regular basis.
- Para 27(a)** ☐ System for regular reporting of operational risks to the board and senior management
- Para 29** ☐ Risk system must link controls to risks
- Para 30** ☐ Control Assessments – must be measured for both design effectiveness and actual operating effectiveness

Uplift

- Para 24** ☐ Ensure Operational risks are segmented into below: legal risk, regulatory risk, compliance risk, conduct risk, technology risk, data risk, reputational risk and change management risk *at minimum*

Clause	CPS230 Requirement	Identification of Areas to Test
11 (a)	effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12(a)	maintain its critical operations within tolerance levels through robust disruption;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12 (b)	manage the risks associated with the use of service	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12	must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external groups and events	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must, to the extent practicable, prevent disruption to critical operations, adapt processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly after a disruption is over;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
14	must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks.	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Risk management framework		
15 (a)	governance arrangements for the oversight of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-15	internal controls that are designed and operating effectively for the management of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	business continuity plan(s) (BCP) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with senior but plausible scenarios;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	processes for the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	As part of the required review of the risk management framework under CPS 230 and SP 135, an APRA-regulated entity must review its operational risk management. The review must cover the aspects of operational risk management set out in paragraph 15.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	Operational risk management must be integrated into an APRA-regulated entity's overall risk management framework and processes. Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's financial contingency planning.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
17	Where APRA considers an APRA-regulated entity's operational risk management has material weaknesses, APRA may require further information/action.	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Role of the Board		
18	The board of an APRA-regulated entity is ultimately responsible for the oversight of an entity's operational risk management, including business continuity and management of service provider arrangements.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
19	The board must ensure that the APRA-regulated entity sets clear roles and responsibilities for senior staff for operational risk management, including business continuity and management of service provider arrangements.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness

Enhancements to:



Operational Risk management

NEW

Para 25

- ☐ Technology Risk – Regular monitoring of age and health of its information assets
 - ☐ Maintained list of Information Assets
 - ☐ Record purchase date & age of Information Assets
 - ☐ Regular monitoring of health of Information Assets
 - ☐ Risks raised for any aging technology

Clause	CPS230 Requirement	Statement of Assurance
11 (a)	effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12 (a)	maintain its critical operations within tolerance levels through severe disruptions;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12 (b)	manage the risks associated with the use of service providers;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external groups and events;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must, to the extent practicable, prevent disruption to critical operations, adjust processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly after a disruption is over;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
14	must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Risk management framework		
15 (a)	governance arrangements for the oversight of operational risk;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	internal controls that are designed and operating effectively for the management of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	business continuity plan(s) (BCP) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with senior but plausible scenarios;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	processes for the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	As part of the required review of the risk management framework under SP1.22 and SP1.23, an APRA-regulated entity must review its operational risk management. The review must cover the aspects of operational risk management set out in paragraph 15.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	Operational risk management must be integrated into an APRA-regulated entity's overall risk management framework and processes. Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's financial contingency planning.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
17	Where APRA considers an APRA-regulated entity's operational risk management has material weaknesses, APRA may require further information/action.	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Role of the Board		
18	The Board of an APRA-regulated entity is ultimately responsible for the oversight of an entity's operational risk management, including business continuity and management of service provider arrangements.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
19	The Board must ensure that the APRA-regulated entity sets clear roles and responsibilities for senior staff for operational risk management, including business continuity and service provider arrangements.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness

Enhancements to:



Operational Risk management

NEW

Para 30 & 31 ☐ System for remediation of material weakness

- ☐ Regularly test controls for design & operating effectiveness
- ☐ Identify any control gaps, weaknesses or failures
- ☐ Document remediation plans with accountabilities and root cause identified

NEW

Para 32 ☐ System of identifying Incidents & Near misses

- ☐ Record any incidents or near misses
- ☐ Implement process for APRA notification of Incidents
- ☐ Ensure details of Incidents/near misses are available during risk assessments/control assessments

Clause	CPS230 Requirement	Identification of Areas to Test
11 (a)	effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12 (a)	maintain its critical operations within tolerance levels through severe disruptions;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13 (a)	manage the risks associated with the use of service providers;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external groups and events;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must, to the extent practicable, prevent disruption to critical operations, adjust processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly after a disruption (a plan);	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
14	must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Risk management framework		
15 (a)	governance arrangements for the oversight of operational risk;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-15	internal controls that are designed and operating effectively for the management of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	business continuity plan(s) (BCP) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with events but disaster scenarios;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	processes for the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	As part of the required review of the risk management framework under CPS 230 and SP1 335, an APRA-regulated entity must review its operational risk management. The review must cover the aspects of operational risk management set out in paragraph 15;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	Operational risk management must be integrated into an APRA-regulated entity's overall risk management framework and processes. Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's financial contingency planning;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
18	Where APRA considers an APRA-regulated entity's operational risk management has material weaknesses, APRA may require further information/action;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Role of the Board		
18	The Board of an APRA-regulated entity, is ultimately responsible for the oversight of an entity's operational risk management, including business continuity and management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
18	The Board must ensure that the APRA-regulated entity sets clear roles and responsibilities for service providers for operational risk management, including business continuity and management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness

Enhancements to:



Business Continuity Planning

Para 34

- ☐ Maintain List of Critical Operations
- ☐ Maintain BCP for every critical operations

APRA Powers

Clause	CPS230 Requirement	Standard of Assessment
11 (a)	effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
11 (b)	maintain its critical operations within tolerance levels through severe disruptions;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
11 (c)	manage the risks associated with the use of service providers;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12	must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external groups and events;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must, to the extent practicable, prevent disruption to critical operations, adapt processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly after a disruption is over;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
14	must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Risk management framework		
15 (a)	governance arrangements for the oversight of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (c)	internal controls that are designed and operating effectively for the management of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (d)	appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (e)	business continuity plans (BCPs) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with service providers;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (f)	processes for the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	As part of the required review of the risk management framework under CPS 230 and SP1 335, an APRA-regulated entity must review its operational risk management. The review must cover the aspects of operational risk management set out in paragraph 15;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
17	Operational risk management must be integrated into an APRA-regulated entity's overall risk management framework and processes. Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's financial contingency planning;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
18	Where APRA considers an APRA-regulated entity's operational risk management has material weaknesses, APRA may require further information/action;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Role of the Board		
19	The Board of an APRA-regulated entity is ultimately responsible for the oversight of an entity's operational risk management, including business continuity and management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
20	The Board must ensure that the APRA-regulated entity sets clear roles and responsibilities for senior staff for operational risk management, including business continuity and service provider management arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness

Critical Operations

35. **Critical operations** are processes undertaken by an APRA-regulated entity or its service provider which, if disrupted beyond tolerance levels, would have a material adverse impact on its depositors, policyholders, beneficiaries or other customers, or its role in the financial system

36. An APRA-regulated entity must, at a minimum, classify the following business operations as critical operations, unless it can justify otherwise:

- (a) for an ADI: payments, deposit-taking and management, custody, settlements and clearing;
- (b) for an insurer (general, life, private health): claims processing;
- (c) for an RSE licensee: investment management and fund administration; and
- (d) for all APRA-regulated entities: customer enquiries and the systems and infrastructure needed to support critical operations..

Enhancements to:



Business Continuity Planning

Para 34

- ☐ Maintain List of Critical Operations
- ☐ Maintain BCP for every critical operations

APRA Powers

NEW

Para 38 & 39

- ☐ Management of Tolerance Levels
 - ☐ Set MAO, RPO and minimum service Levels required for critical operations
 - ☐ APRA may set tolerance levels for an APRA regulated entity

APRA Powers

NEW

Para 44

- ☐ System of Testing of BCP's
 - ☐ Generate list of **severe but plausible scenarios**
 - ☐ Test activation of BCM in scenarios

APRA Powers

Clause	CPS230 Requirement	Statement of Assurance
11 (a)	effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12 (a)	maintain its critical operations within tolerance levels through severe disruptions;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12 (b)	manage the risks associated with the use of service providers;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external groups and events;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
14	must, to the extent practicable, prevent disruption to critical operations, adjust processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly after a disruption is over;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15	must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Risk management framework		
15 (a)	governance arrangements for the oversight of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (c)	internal controls that are designed and operating effectively for the management of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (d)	appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (e)	business continuity plan(s) (BCP) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with severe but plausible scenarios;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (f)	processes for the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	As part of the required review of the risk management framework under CPS 230 and CPS 231, an APRA-regulated entity must review its operational risk management. The review must cover the aspects of operational risk management set out in paragraph 15;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
17	Operational risk management must be integrated into an APRA-regulated entity's overall risk management framework and processes. Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's financial contingency planning;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
18	Where APRA considers an APRA-regulated entity's operational risk management has material weaknesses, APRA may require further information/action;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Role of the Board		
19	The board of an APRA-regulated entity is ultimately responsible for the oversight of an entity's operational risk management, including business continuity and management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
20	The board must ensure that the APRA-regulated entity sets clear roles and responsibilities for service providers for operational risk management, including business continuity and management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness

Enhancements to:



Business Continuity Planning

NEW

Para 42

☐ BCP Activation

☐ Add a “APRA Notification” Step after suffered a disruption to a critical operation outside tolerance.

Clause	CPS230 Requirement	Identification of Areas to Assess
11 (a)	effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12 (a)	maintain its critical operations within tolerance levels through severe disruptions;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13 (a)	manage the risks associated with the use of service providers;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external groups and events;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must, to the extent practicable, prevent disruption to critical operations, adapt processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly after a disruption is over;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
14	must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Risk management framework		
15 (a)	governance arrangements for the oversight of operational risk;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-13	internal controls that are designed and operating effectively for the management of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	business continuity plan(s) (BCP) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with senior but plausible scenarios;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	processes for the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	As part of the required review of the risk management framework under CPS 230 and SP1 335, an APRA-regulated entity must review its operational risk management. The review must cover the aspects of operational risk management set out in paragraph 15.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	Operational risk management must be integrated into an APRA-regulated entity's overall risk management framework and processes. Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's financial contingency planning.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
18	Where APRA considers an APRA-regulated entity's operational risk management has material weaknesses, APRA may require further information/action.	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Role of the Board		
18	The Board of an APRA-regulated entity is ultimately responsible for the oversight of an entity's operational risk management, including business continuity and management of service provider arrangements.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
18	The Board must ensure that the APRA-regulated entity sets clear roles and responsibilities for senior staff for operational risk management, including business continuity and service management arrangements.	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness

5

Enhancements to:



Business Continuity Planning

Key Concerns

- Determining Critical Operations
- Lack of End to End process mapping

Recommendations

- Focus on operations that directly affect your end consumer
- Breaking down in smaller operations to better define critical operations

Enhancements to:



Management of Service Providers

Para 49-52

☐ Manage Material Service Providers

☐ Maintain register of material service providers and associated risks

☐ Submit Register to APRA on annual basis

Clause	CPS230 Requirement	Standard of Assessment
11-12	effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12-13	maintain its critical operations within tolerance levels through severe disruptions;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13-14	manage the risks associated with the use of service providers;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
14	must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external groups and events;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15	must, to the extent practicable, prevent disruption to critical operations, adapt processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly after a disruption is over;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Risk management framework		
17-18	governance arrangements for the oversight of operational risk;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
18-19	an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
19-20	internal controls that are designed and operating effectively for the management of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
20-21	appropriate monitoring, analysis and reporting of operational risks and escalation processes for operational incidents and events;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
21-22	business continuity plans (BCPs) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with senior but plausible scenarios;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
22-23	processes for the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
23	As part of the required review of the risk management framework under CPS 230 and SP 133, an APRA-regulated entity must review its operational risk management. The review must cover the aspects of operational risk management set out in paragraph 15;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
24	Operational risk management must be integrated into an APRA-regulated entity's overall risk management framework and processes. Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's financial contingency planning;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
25	Where APRA considers an APRA-regulated entity's operational risk management has material weaknesses, APRA may require further information/action;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Role of the Board		
26	The Board of an APRA-regulated entity is ultimately responsible for the oversight of an entity's operational risk management, including business continuity and management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
27	The Board must ensure that the APRA-regulated entity sets clear roles and responsibilities for senior staff for operational risk management, including business continuity and management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness

Material Service Providers

49. **Material service providers** are those on which the entity relies to undertake a critical operation or that expose it to material operational risk. **Material arrangements** are those on which the entity relies to undertake a critical operation or that expose it to material operational risk.

50. An APRA-regulated entity must, at a minimum, classify a provider of the following services as a material service provider, unless it can justify otherwise:

- (a) for an ADI: credit assessment, funding and liquidity management and mortgage brokerage;
- (b) for an insurer (general, life, private health): underwriting, claims management, insurance brokerage and reinsurance;
- (c) for an RSE licensee: fund administration, custodial services, investment management and arrangements with promoters and financial planners; and
- (d) for all APRA-regulated entities: risk management, core technology services and internal audit.

Enhancements to:



Management of Service Providers

Para 49-52

- ☐ Manage Material Service Providers
 - ☐ Maintain register of material service providers and associated risks
 - ☐ Submit Register to APRA on annual basis

Uplift

Para 47 & 48

- ☐ Update Service Provider Management Policy
 - ☐ Cover arrangement for critical operations AND any that expose organisation to material operational risk
 - ☐ Cover risks associated with 4th Parties

Uplift

Para 58 & 60

- ☐ Update Service Agreements with specified inclusions
- ☐ Conduct regular internal Audits on providers compliance with service agreements
- ☐ Regular reporting to Board on Service Provider performance

Clause	CPS230 Requirement	Identification of Areas to Assess
11 (a)	effectively manage its operational risks, and set and maintain appropriate standards for conduct and compliance;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12 (a)	maintain its critical operations within tolerance levels through severe disruptions;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12 (b)	manage the risks associated with the use of service providers;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
12	must identify, assess and manage operational risks that may result from inadequate or failed internal processes or systems, the actions or inactions of people or external groups and events;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
13	must, to the extent practicable, prevent disruption to critical operations, adjust processes and systems to continue to operate within tolerance levels in the event of a disruption and return to normal operations promptly after a disruption (a plan);	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
14	must not rely on a service provider unless it can ensure that in doing so it can continue to meet its prudential obligations in full and effectively manage the associated risks;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Risk management framework		
15 (a)	governance arrangements for the oversight of operational risk;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15 (b)	an assessment of its operational risk profile, with a defined risk appetite supported by indicators and limits;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	internal controls that are designed and operating effectively for the management of operational risks;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	appropriate monitoring, analysis and reporting of operational risks and incident processes for operational incidents and events;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	business continuity plan(s) (BCP) that set out how the entity would identify, manage and respond to a disruption within tolerance levels and are regularly tested with senior but plausible scenarios;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
15-16	processes for the management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	As part of the required review of the risk management framework under CPS 230 and CPS 231, an APRA-regulated entity must review its operational risk management. The review must cover the aspects of operational risk management set out in paragraph 15;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
16	Operational risk management must be integrated into an APRA-regulated entity's overall risk management framework and processes. Business continuity planning must be consistent with, and not conflict or undermine, an APRA-regulated entity's financial contingency planning;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
18	Where APRA considers an APRA-regulated entity's operational risk management has material weaknesses, APRA may require further information/action;	<input type="checkbox"/> Risk system must link controls to risks <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness <input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
Role of the Board		
18	The Board of an APRA-regulated entity is ultimately responsible for the oversight of an entity's operational risk management, including business continuity and management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness
18	The Board must ensure that the APRA-regulated entity sets clear roles and responsibilities for senior staff for operational risk management, including business continuity and management of service provider arrangements;	<input type="checkbox"/> Controls should be measured both design effectiveness & actual operating effectiveness

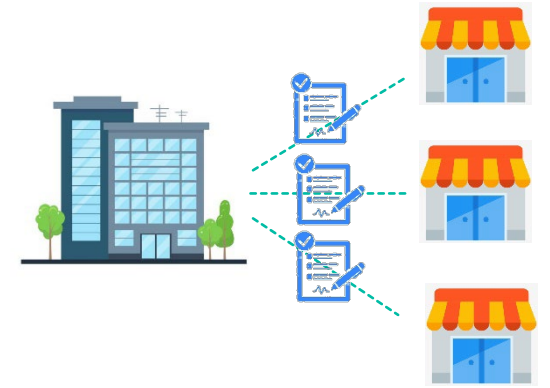
3 Contractual Changes to Service Provider Agreements

In Service Arrangements (Clause 54)

- ✓ services and service levels
- ✓ rights, responsibilities, and expectations of each party
- ✓ ability of the entity to meet its legal and compliance obligations;
- ✓ require notification by the service provider of its use of other material service providers, through sub-contracting or other arrangements;
- ✓ require the liability for any failure on the part of any sub-contractor to be the responsibility of the service provider
- ✓ include a force majeure provision indicating those parts of the contract that would continue in the case of a force majeure event;
- ✓ termination provisions for right to terminate

Provisions for APRA (Clause 55)

- ✓ Allow APRA access to documentation, data and any other information related to the provision of the service
- ✓ Allow APRA the right to conduct an on-site visit to the service provider

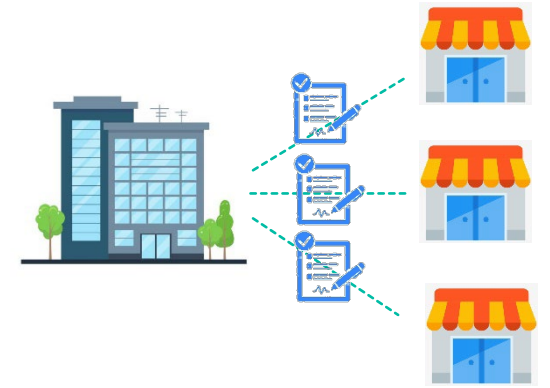


**At next Contract
renewal *or*
before 1 July 2026**

Enhancements to:



Management of Service Providers



Key Concerns

- Difficulty in negotiating/obtaining info from larger service providers
- Embedding APRA clauses into service agreements
- Extra work required for quantity of material service providers
- Identifying material service providers (e.g. brokers)

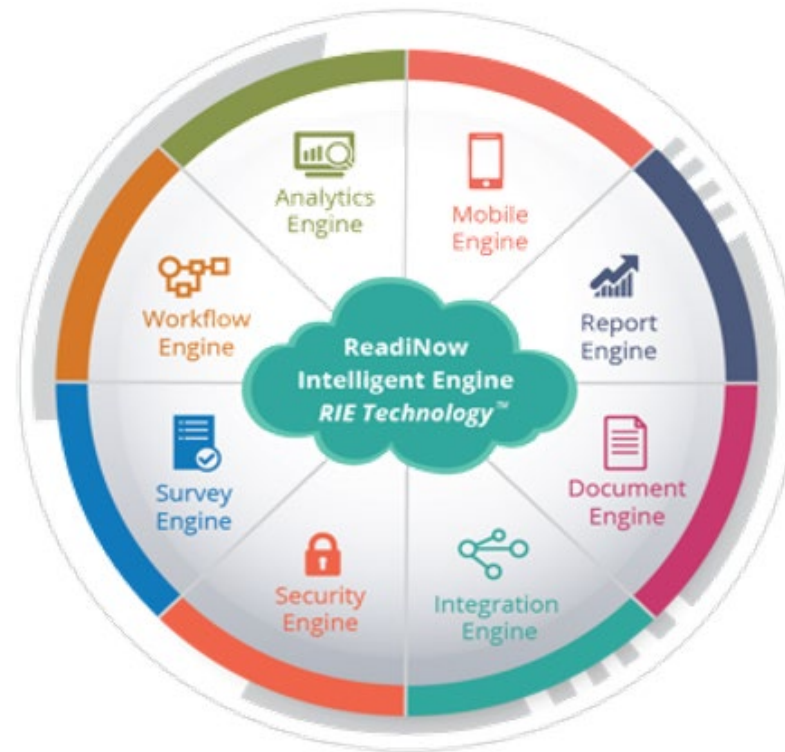
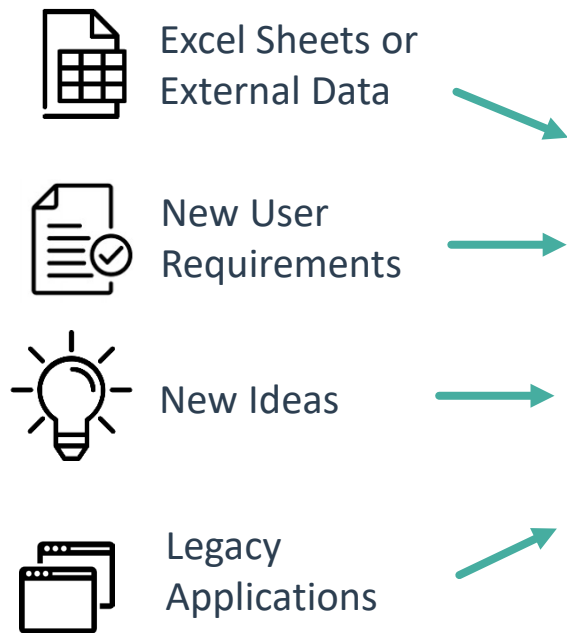
Recommendations

- Vendor Education – providing guidance documents to vendors
- Tiering of Material service providers
- Documenting approach and justification for APRA
- Continuously reviewing vendor materiality due to potential changes in vendor relationships.
- Resource planning for vendor management

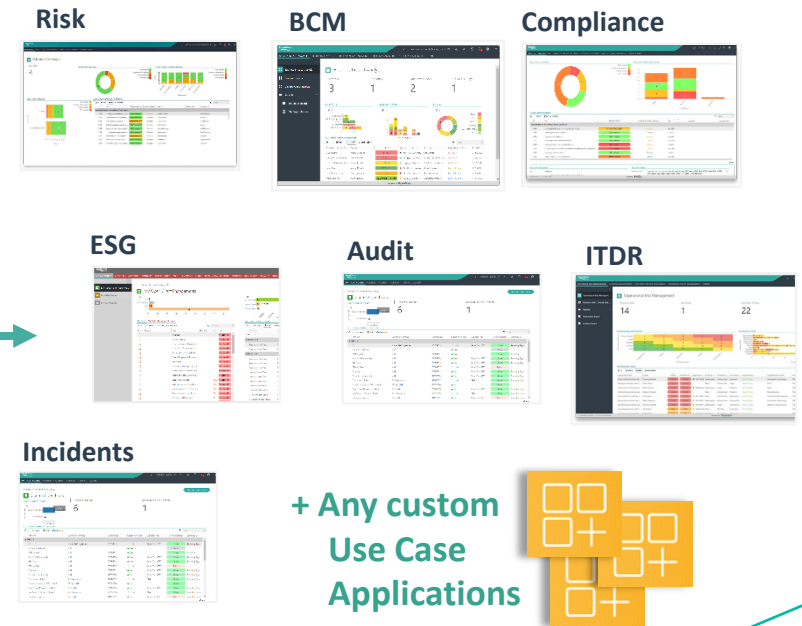
What is ReadiNow

What is ReadiNow


ReadiNow **No-Code** Drag & Drop




Transform or Build Unlimited Use Cases




Governance, Risk & Compliance




BCM




Risk




Compliance




Audit




Incident




WHS



Vendor



Complaints



Key Indicators

IT/Cyber Solutions



IT Risk



IT Security Incident




ITDR




IT Compliance


Environmental, Social & Governance



Materiality Assessments




Disclosure



Metrics


+ Any custom Use Case Applications




Configurable Forms & Screens




Dashboards




Analytics




Workflow




Mobile




Role Based Security



Document Generation



Alerts & Notifications



Integrations

CPS230 Module

Business Continuity



Critical Operations



Testing Program



Recovery Actions



Risk Management



Risk Assessment



Control Assessment



Risk Taxonomy



Incident Management



Incident & Near Misses



Reporting



Indicators



Service Provider Management



Vendor Register



Contract Management



Due Diligence



Configurable
Forms & Screens



Dashboards



Analytics



Workflow



Mobile



Role Based
Security



Document
Generation



Alerts &
Notifications

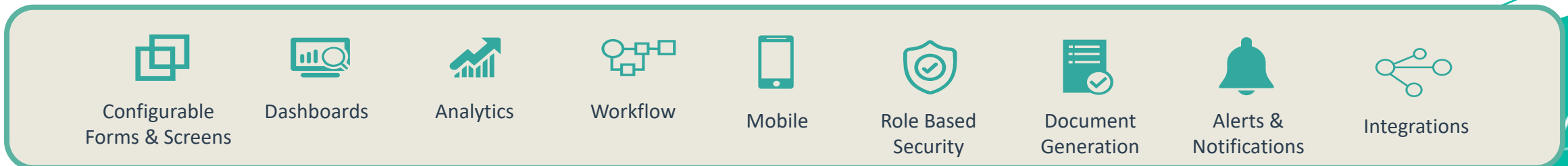


Integrations

CPS230 Module



- ✓ Manage all your CPS230 requirements
- ✓ Auto-generate APRA notification reports
- ✓ Executive-Level Insights with real-time CPS230 dashboards for Management and Board reporting
- ✓ Leverage no-code automation for effortless control of Risk, Business Continuity, Incident and Vendor Management.



Live Demo