



Introduction and agenda

01

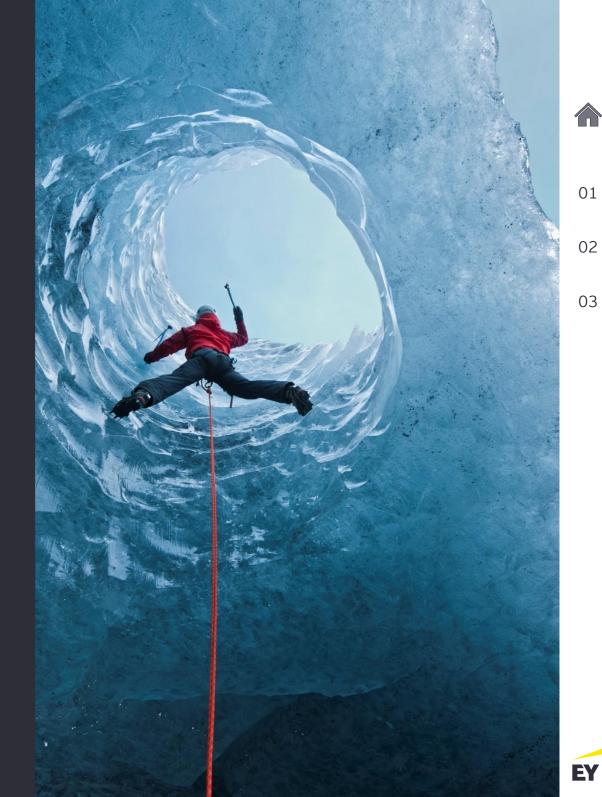
Key features

02

Key challenges

03

Actions to be taken









Why are regulators focused on operational risk and resilience?



Operational risk and resilience have become a common focus area of regulators in the global markets.

Higher expectations for enhanced customer experience

Uninterrupted, 24/7 access to products and services

Increased confidence in security and confidentiality of their data

▶ Low tolerance for disruptions

Systemic operational risk failures

- Industry-wide failures in management of operational risk and remediation of known issues (Hayne Royal Commission)
- Greater focus on non-financial risks and increased scrutiny around Senior Management and Board oversight
- Operational risk events leading to capital charges due to poorly-designed and implemented operational risk frameworks

Increased operational complexity susceptible to outages and breaks

Mergers, acquisitions, enforced structural change and growing global entities are increasing the scale and complexity of operations and groups

► Highly-complex and inter-connected operations susceptible to increased operational outages and breaks

Invisible risks reside in voluminous service providers

- ▶ Increasing reliance on service providers
- ► Complex supply chains, i.e. third, fourthparty and intra-group risks
- ► Interconnectedness and substitutability heightened the severity of single point of failure risks in key systems "nodes"

Increased risk of disruptions in legacy systems and during IT modernisations

- Ageing infrastructure and legacy systems prone to outages and posing integration challenges with newer systems and applications
- Managing old legacy systems while delivering large and complex transformation programs brings exposure to the risk of disruptions



02



Key changes

As global regulations start to align, we begin to see similarities with the UK operational resilience framework, the US Federal Reserve and the European Commission in the approach they are taking to Operational Resilience.

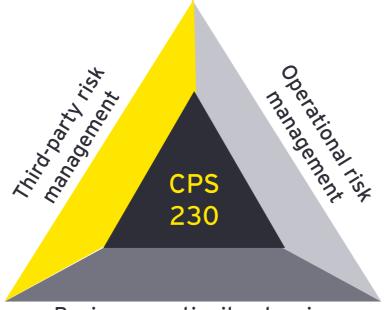
On 28th July, APRA released the draft Prudential Standard CPS 230 which consolidates the prudential standards CPS 231 Outsourcing and CPS 232 Business Continuity Management, but more importantly raises the bar on

operational risk management practices.

Third parties

Now applies to 'Material Service Providers', capturing a broader range of third parties compared to 'outsourced' material business activities

CPS 231 will be superseded by **CPS 230**



Business continuity planning

Business continuity planning

The focus is on critical operations and minimising disruptions to them

CPS 232 will be superseded by CPS 230

01

02

03

Operational risk

No previous operational risk standard

Operational risk only covered as part of CPS 220 requirements

No previously articulated requirements for controls



Key features from APRA's draft standard



Business-line management, rather than risk management functions, are responsible for the oversight and management of operational risk.

01

02

UZ

03

For critical operations, an end-toend process map will be required, as well as the mapping of key dependencies on people, processes, technology and third parties.

Financial safety

Critical Operations

Board

and SM

Material Service Providers

Tolerances Levels

Risk Profiles, Control Testing, and Monitoring

Financial system

stability

diligence procedures for each material service provider. Properly defined and monitored contract requirements will also be required.

Entities will be required to

establish appropriate due

Tolerance levels must be distinct from risk appetites/RTOs, be expressed referencing customer outcomes and

metrics.



Customers and markets

Critical operations, their processes, risks and controls have to be documented, monitored, analysed and reported. Control weaknesses and incidents should act as feeds to update risk profiles.



What is APRA looking for?



01

02

03

Board is ultimately accountable for oversight of operational risk. Business is responsible.

Use scenario analysis to assess severe operational risk events and identify control weaknesses and new or amended controls.

Regularly monitor, review

and test controls for

design and operating

effectiveness. Frequency

driven by materiality of

risk.

Strengthen

Operational Risk Management

Maintain effective internal controls to manage operational risk profile within appetite.

Document E2E processes to deliver critical operations. Perform ongoing monitoring, analytics and reporting of operational risks.

Risk profile to be updated

with incidents and issues.

Expected impact on risk

profile for new products, services, geographies and technologies.



What is APRA looking for?



01

02

03

operations, set tolerances to define levels of disruption, and maintain credible plans to respond to and recover from incidents and events

Identify critical

Improve Business Continuity Planning

Testing program covering all critical operations and includes an annual exercise with a range of severe but plausible scenarios that could impact critical operations

Critical operations
definition focused on
outcomes and the key
stakeholders/customers
of the entity rather than
the entity itself

BCP must set out how to recover critical operations within tolerance levels in the event of a severe but plausible disruption

Set Board-approved customer and outcomesfocused tolerance levels for each of the critical operations

submit the BCP to APRA annually, and notify APRA within 24 hours, of a material disruption to a critical operation or if the BCP has been activated

What is APRA looking for?



01

02

03

Identify material service providers and manage the risks associated with the use of these providers

All arrangements to be formalised through a legal agreement, including provisions to allow APRA to conduct on-site visits and access to service-related documentation

Notify APRA not more than 20 business days, after entering into or materially changing an agreement for the provision of a service to undertake a critical operation Enhance third-party risk management

Third party arrangements to ensure risks to ongoing service provision are managed, BCP can be executed, and orderly exit can be arranged A Board-approved policy
for managing risks
associated with reliance on
service providers. The
policy should also set out
the approach for
managing risks with fourth
parties

Submit the material service providers inventory/register to APRA on an annual basis and monitor effectiveness of risk with use of service provider









Challenges

Although many entities have standalone frameworks covering Operational risk, Business Continuity Planning, Disaster Recovery and Third-Party Risk Management which are directionally consistent with the Standard, this siloed approach is no longer sufficient. Focus is now shifting to resilience over end-to-end processes which need to enable operational endurance over an extended period, but also be robust to prevent service disruptions.



01

Lack of engagement or challenge at Board level

- ▶ Lack of a clear Board-driven risk appetite, making it hard to determine true effectiveness of key controls
- ▶ Poor quality information or lack understanding by Board members of technical details

02

Lack of coordination and oversight

- ▶ Limited Business and/or IT buy-in to Resilience programmes
- ▶ Siloed teams for Business Continuity, Disaster Recovery and Third-party Risk Management.-
- ▶ Ineffective challenge by Boards, senior management as well as second and/or third line functions.

03

Inefficiencies in the control environment

- ▶ Inefficient/duplicative and inconsistent control testing activities across the 3LoD and teams
- ▶ Inadequate frameworks, responsibilities, tools and enablers to manage the controls taxonomies and libraries
- ▶ Limited understanding of third-party owned and operated controls

Multiple change programs

- ► Complex, overlapping change programmes make it hard to identify where potential weaknesses are in controls and core systems
- ▶ Resilience requirements are not built-in to product, process and system design governance and controls
- ▶ **Technology and data changes** are not tested robustly enough pre-implementation

Limited focus on continuity of critical operations

- ▶ **Mediocre mapping of internal dependencies and systems**, and understanding of external dependencies and third-partis. Updates to mapping are infrequent.
- ► Lack of understanding (and testing) of manual work-arounds or continuity arrangements for business processes for when systems or third parties fail

Inadequate testing of capabilities

- ▶ Testing of Business Continuity, ITDR and Work Area Recovery plans is component-based, leaving gaps.
- ► Tests are designed to 'test for green' meaning that they do not consider real life scenarios based on potential impact of disruption
- ▶ Third parties and ecosystem participants are not included in testing, leaving gaps that are identified in incidents





03

Insights from recent industry roundtable

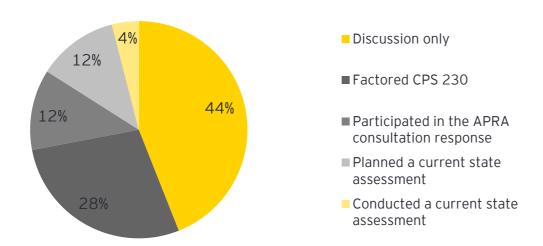


EY recently hosted an industry roundtable on CPS 230 attended by a cross section of CAEs from regulated entities in the Australian financial services sector. The roundtable gauged CAE views on key challenges and the likely response and role of internal audit functions.

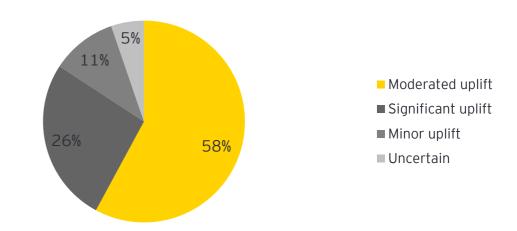
- 01
- ▶ 12% of Internal Audit functions have already factored CPS 230 related reviews into their internal audit plans. Only 12% of CAEs in attendance participated in the response to APRA's consultation on CPS 230.
- 02

▶84% of CAEs believe that a moderate to significant uplift in capabilities will be required to demonstrate full compliance with the standard.

What activities have IA conducted in relation to CPS 230 to date



How much uplift is needed in your organisation to meet the requirements of the draft CPS 230





Insights from recent industry roundtable

What do you think internal audit's role should be in meeting the requirements of CPS 230?



01

02

03

Readiness assessment

Assess readiness - Regulatory impact assessment

Began factoring it into audit planning

Gap Analysis readiness assessment

Readiness

Hold business to account

Assessment of implementation plans

Have a clear audit plan that provides sufficient DE and OE coverage of key controls supporting obligations

Assurance over the implementation



Insights from recent industry roundtable

What do you think internal audit's role should be in meeting the requirements of CPS 230?



01

02

03

Readiness reviews, integrated with existing 231-232 during transition

Readiness and ability deliver to meet timeline

Resourcing and capability review

Plan audit for 24 and be part of the transition team

Provide audit insights on gaps to remediate based on historical audit work performed Maturity assessment capability assessment
(3 line of defences)

Ensuring end-to-end processes are completely mapped. Risks and controls to be identified as they relate to 3rd/4th party dependencies, BCP, etc., and included in specific reviews

Readiness assessment, share information for end-to-end processing. Consider overall harmony of distinct silos input

Helping the business create cross-functional linkage and dependencies



02

01

03

Responsibilities across the 3LoD



First, Second, and Third line of Defense are coming together to jointly deliver and enable resilience across the enterprise

Enterprise Resilience Function

- Responsible for day-to-day planning and management of resilience program and implementation
- Perform crisis management planning, testing and management
- Measure and report on resilience program maturity and performance

Business and Operations

- Identify and prioritize critical business services
- Perform business continuity management
- Design, implement and test controls to enable continuity of business services under different operating environments

Technology

- Provide enabling technology solutions to ensure delivery of critical business services
- Manage disaster recovery and cyber resilience program
- Design, implement and test controls to enable continuity of business services under different operating environments

Risk and Compliance

- Define and monitor compliance to resilience policy and standards
- ▶ Review and challenge effectiveness of plans and capabilities
- Provide reporting on risks to the firm's resilience to Board and Committees

3

Internal Audit

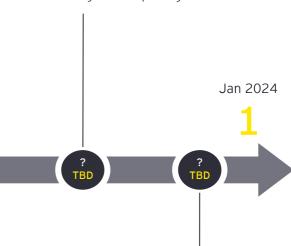
- Provide independent validation of resilience program and capabilities, including associated process and controls
- Provide input or review of design effectiveness and maturity of resilience program



Roadmap for the business and IA

- Actions where IA could play a role are **bolded**.
- ▶ IA should also ensure that audits covering topics contained within CPS 230 (e.g., CPS 231 and 232) are performed with an eye on the future requirements.
- 1. Identify critical operations
 - APRA's initial list of critical operations are a good starting point, but are not necessarily exhaustive
- 3. Identify material service providers
 - Develop third-party risk profiling and assessment program based on an established inventory
 - Re-visit contractual obligations to obtain transparency on thirdparty operated controls

- 5. Clearly define ownership
 - Set out roles, responsibilities and accountability
 - Consider the impact on the Banking Executive Accountability Regime (BEAR) and Financial Accountability Regime (FAR)
- 7. Analyse, monitor and report
 - Determine analysis methods for risk data
 - Provide appropriate Board and Senior Management reporting



28

Jul 2022

- 2. Document critical end-to-end business processes
 - Document critical processes to understand end-to-end data flows, systems, applicable operational risks, handoffs regulatory obligations and control instances.
- 4. Establish tolerances levels
 - Board approved acceptable levels of impact/outage for processes and systems
 - Ensure tolerance levels are 'customer' and 'outcomes'- focused

- 6. Review and test internal controls regularly
 - Develop an end-to-end internal controls testing program across the 3LOD (combined assurance)
 - Identify resilience issues within the current environment (e.g., single points of failure)

- . Update risk profile
 - Evaluate approach to keeping the operational risk profiles from GRC tool data up to date. Data includes incidents, control weaknesses, potential changes from products, digitisation and modernisation, processes and technology that can have a material impact on the profile



01

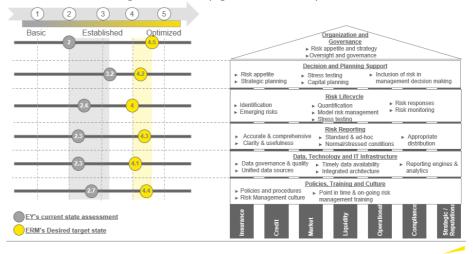
02

Operational risk framework diagnostic

- Perform a current state assessment of operational risk maturity against recent regulatory expectations and latest industry trends.
- 2. Compare the current state against minimum standards and any future defined target state.
- 3. For the gaps between the current state and target state, prioritise and sequence the key framework enhancements to provide greater value to the business, information to the board, and enable critical services to be more resilient for stakeholders.
- 4. Update the maturity model on a regular basis and perform current state assessment on targeted areas of business to identify if capabilities meet expectations.

Level	Level 2	Level	Level 4	Level 5.			
.0		,					
Basic	cMaturit g Level D	Established	cMaturi tg Level 45	Optimized	Rating (1-5)	Mean of ERM Component Subsection	Mean for EFR component
There is a basic operational risk framework document which has not been approved outside of second/third line of defense.		A formally-documented operational risk management framework has been approved by Senior Management and Board. The framework is reviewed and updated on an advice busit. The framework is amended and applied differently in each business with.		A formally-documented operational risk management framework has been approved by Sosion Management and Board. The framework insign with the ERM framework in Framework is reviewed and updated on a regular basis. The framework is explicit exterprise-wide and cover all material operations, including geographics, corporate functions and material subsidiaries and joint ventures.	5		
The operational risk framework covers risk identification and assessment methods.		The operational risk framework covers most of RCSA, KRIs, Loss event/hear misses, scenario analysis and issue tracking.		The operational risk framework covers all of RCSA, KRIs, Loss weathers misses (internal incidence), occuratio analysis. Issue tracking, acturated loss or exercise and exposure operatifications and a just odes with all regulatory requirements. The framework express that the components work together constrictivity using zeron enthods, wording tracemente, assessments etc. and align with ERM methodologics, woordings atts.	2		
There is no Board-created enterprise level rick committee for overseeing all risks, only an Audit Committee which considers risks as well.		There exists a Board-level enterprise level risk committee for overseeing all risks, to which a operational risk committee resports. Committee meetings are be held on an es-needed basis and without adequate time and resources to permit proper discussions and desirion-mixther.		There exists a Board-created enterprise level risk committee for overseeing all risks, to which an operational risk committee reports. Committee mostings are hold at appropriate frequencies with adequate time and resources to permit productive discussion and decision- making.			
The Head of Audit who is responsible for risk management activities as well.		There is a Head of Operational Risk who reports to the CRO. There is a small operational risk department with some experience.		There is a Head of Operational Risk who reports to the CRO. There is an experienced operational risk department who are able to run all aspects of the operational risk framework components (RCSAs, KRIs, Loss Events, Securios etc.)	2		
There is no dedicated operational risk committee. Operational risks are managed by each individual business unit/function		There exists an operational risk committee. The committee lacks a combination of senior members with expertise in business stabilities, fisancial or risk management expertise and independent non-exceptive board members.		The Company's operational risk committee includes a combination of senior members with expertise in business extrition, financial or risk management expertise and independent non-executive board members. Committee meetings are held at appropriate frequencies with adequate time and resources to permit productive discussion and decision- making.	2		
Risk Misagement and internal wells are the sum- function and are not independent (e.g. report to CPO).		There we three distinct lines of defense (1st line is the businesse, 2nd line is list in high reaction inc ERM (MR). Compliance, Legal, business containty ace, that facilitate risk managament in the first line, and the third line is betterall what!) which address most risk types. There is come overlap in responsibilities. There are decaptes politics and procedures which identify respective responsibilities.		There are three distinct lines of discuss around in immageness which address all risk types including those managed by moterial contraversed arrangements. There includes us independent, coordinated EPMI process (linckhalleg convergences of EPMI, compliance, Legal ECM, IT, lefo Sec, Actuarul functions and an independent between Available function. The titler certains are coordinated, work to applicable, layer little certain for the contraverse of	2		
		Operational risk management functions exists in all of the business with and either here a direct or indirect reporting line to the CRO (centralled of decentraliced). Methodologies are not consistent for all functions. BU functions do not report risk information consistently to corporate function.		Operational risk management functions exist in all of the business waits and with above a direct or indirect reporting into the CPO (centralized of decorralized). Methodologies are consistent for all functions. Business functions will have sufficient independence to effectively challege and report on BU pris management republishes and report risk information frought to expenditude on the consistency of the co	2		
There are no official escalation procedures, issues are reported on an ad-hoc basis based on management judgement		There exist escalation procedures within business units/functions, but do not effectively excelled issues and/or unecceptable risk exposures to Senior Management and Bloard		There exists a robust and reliable escalation procedure which appropriately and timely escalates compliance issues, losers, branches in the risk appretic limits or credirect to Sealor Management, Board, op risk committee etc. Escalation points are consistent with risk annetite and associated limits.	2	2.4	
Operational risks are related to compliance with regulations.		Operational risks are related to compliance with regulations, policies and procedures.		A documented process is in place to identify and assess all operational risks, (including energing risks, and legal and compliance risks), using business objectives as the starting point to determine	1		

Based upon the observations made during the current state assessment, ERM program capabilities have been assessed against EY's ERM Framework maturity diagnostic tool and rated accordingly. The chart on the left (below) indicates EY's assessment of the current maturity rating and ERM program's desired target state rating for each capability, as it relates to the six major layers of EY's ERM Framework. While xxx has made much progress in recent years in achieving the current state maturity, significant work remains to achieve the desired target state and move the program from Established to Optimized.





01

02



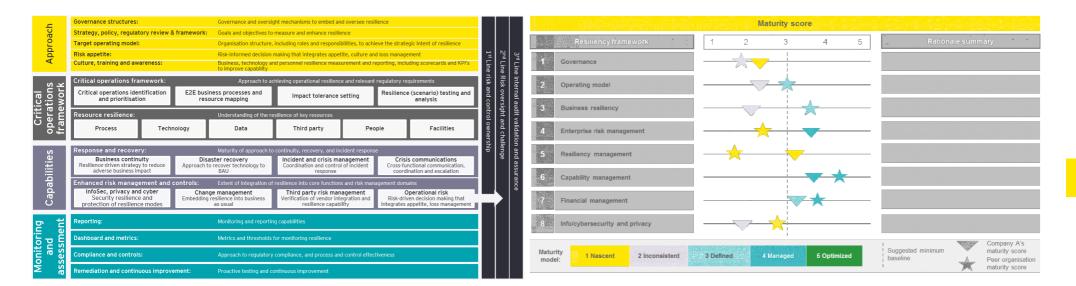
Resilience risk framework diagnostic



01

02

03



Maturity ratings against EY's operational resilience framework

Peer and industry benchmark

Our resilience maturity scale used in our reporting



EY

20 Private and confidential Source: EY Diagnostic Materials

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2022 Ernst & Young, Australia. All Rights Reserved.

Liability limited by a scheme approved under Professional Standards Legislation.



In line with EY's commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

This communication provides general information which is current at the time of production. The information contained in this communication does not constitute advice and should not be relied on as such. Professional advice should be sought prior to any action being taken in reliance on any of the information. Ernst & Young disclaims all responsibility and liability (including, without limitation, for any direct or indirect or consequential costs, loss or damage or loss of profits) arising from anything done or omitted to be done by any party in reliance, whether wholly or partially, on any of the information. Any party that relies on the information does so at its own risk.

ey.com