

CPS 230 - Operational Risk Management: Expectations and Compliance

IIA Financial Services Assurance Forum 2022

24 November 2022

Today's presenters



Damien O'Meara

Partner,
Financial Services Enterprise
Risk and Internal Audit Leader

damien.omeara@au.ey.com



Hanny Hassan

Partner,
Financial Services
Technology Risk and Third
Party Risk Management
Leader

hanny.hassan@au.ey.com



01

02

03

Introduction and agenda

01

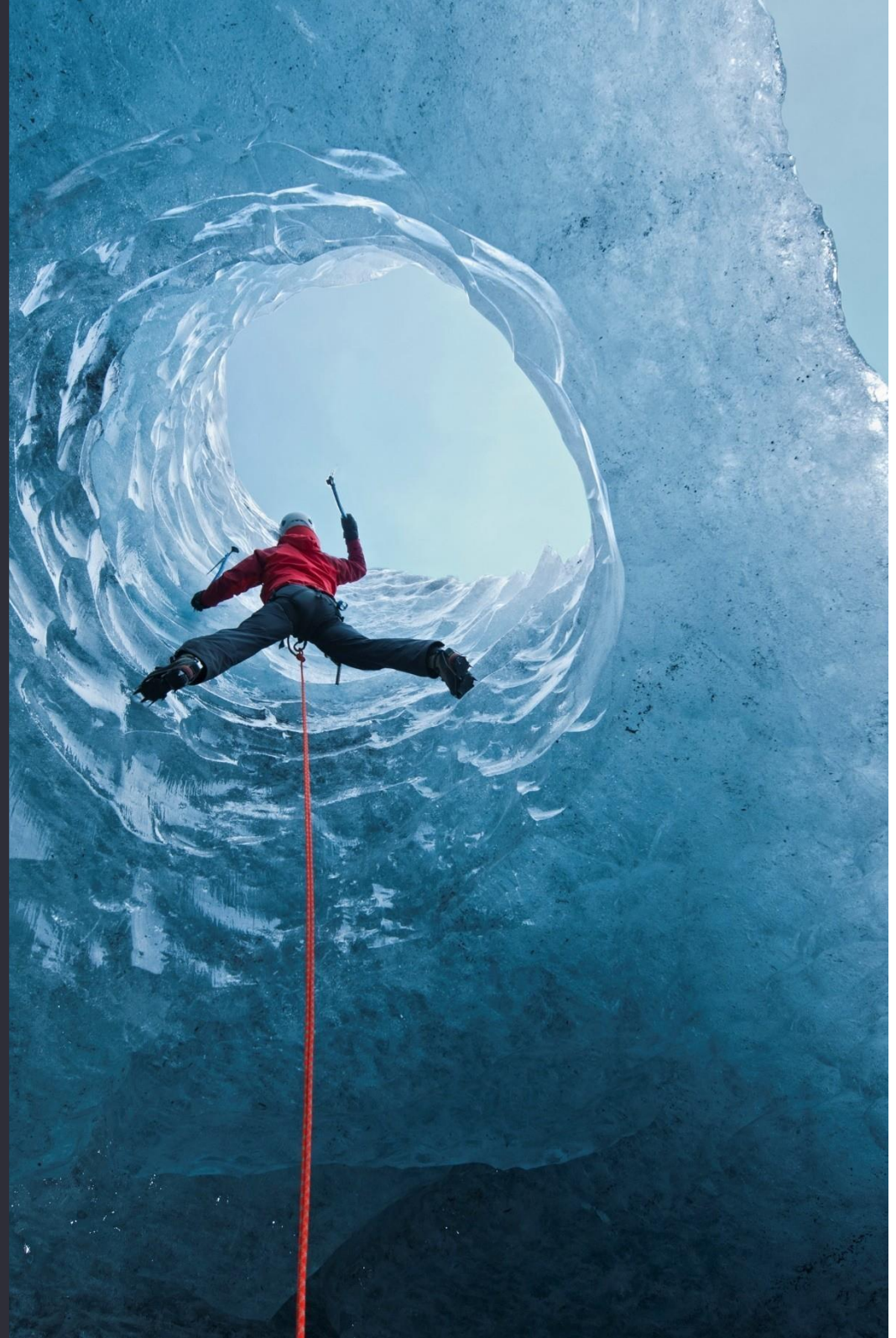
Key features

02

Key challenges

03

Actions to be taken



01

02

03



01

02

03

Key features

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.

01

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

Increased operational complexity susceptible to outages and breaks

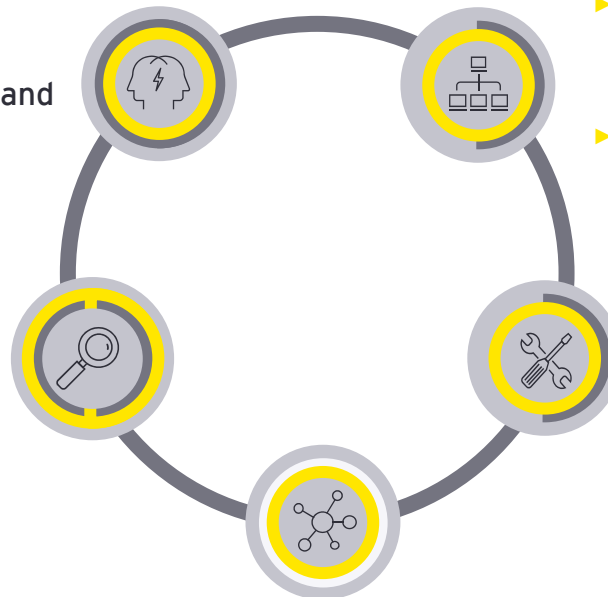
- ▶ Mergers, acquisitions, enforced structural change and growing global entities are increasing the scale and complexity of operations and groups
- ▶ Highly-complex and inter-connected operations susceptible to increased operational outages and breaks

02

03

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 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

Invisible risks reside in voluminous service providers

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

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.

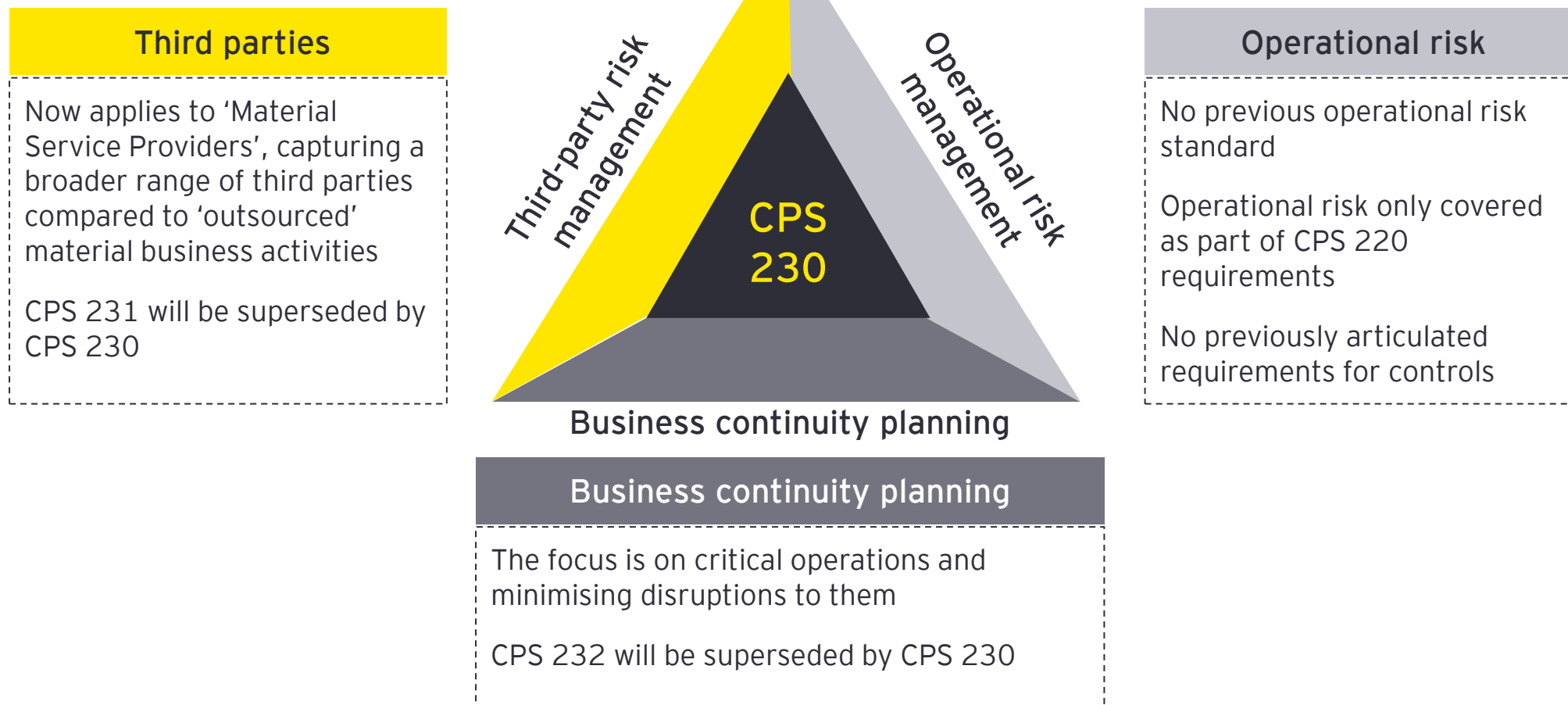
On 28th July, APRA released the draft Prudential Standard CPS 230 which consolidates the prudential standards CPS 231 Outsourcing and CPS 232 Business Continuity Management, but more importantly raises the bar on operational risk management practices.



01

02

03



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.

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

Entities will be required to establish appropriate due diligence procedures for each material service provider. Properly defined and monitored contract requirements will also be required.

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

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.



01

02

03

What is APRA looking for?



01

02

03

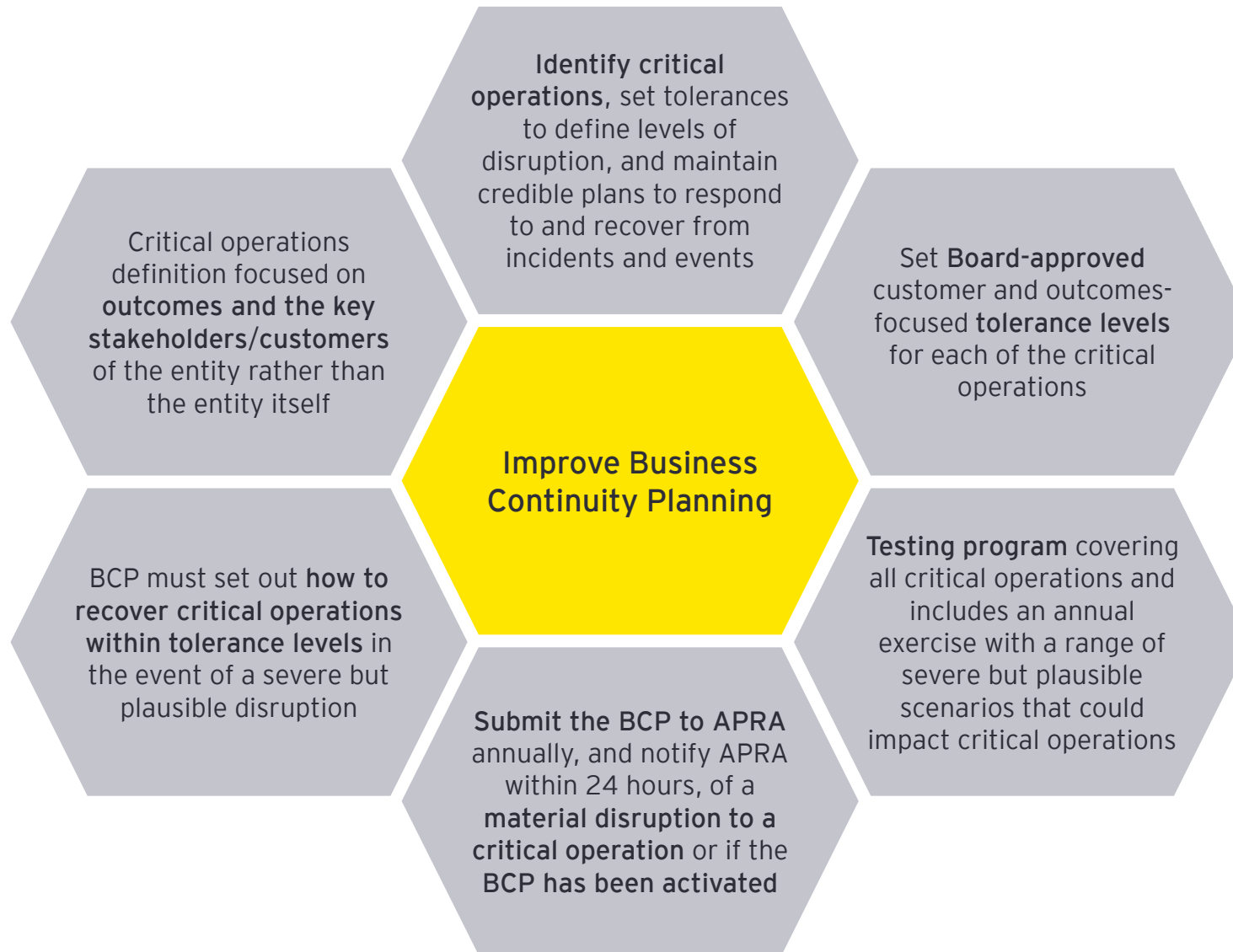
What is APRA looking for?



01

02

03



What is APRA looking for?



01

02

03





01

02

03

Key challenges

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

3

Actions to be taken



01

02

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

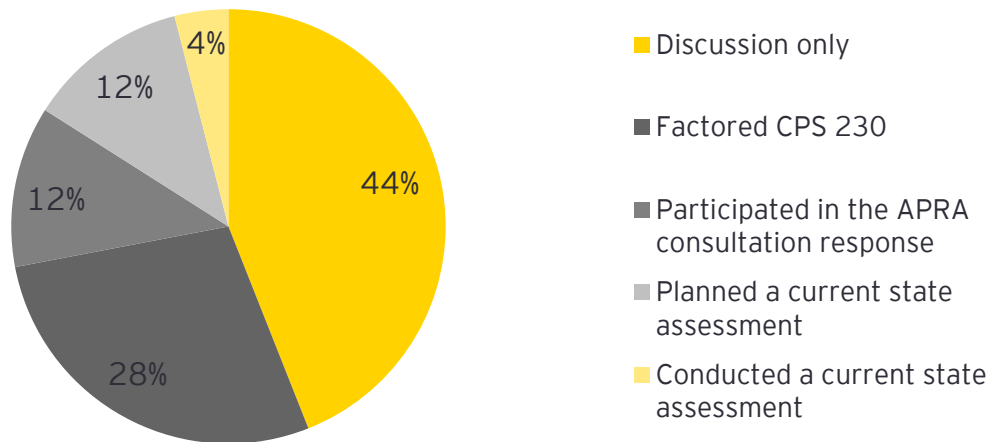
▶ 12% of Internal Audit functions have already factored CPS 230 related reviews into their internal audit plans. Only 12% of CAEs in attendance participated in the response to APRA's consultation on CPS 230.

02

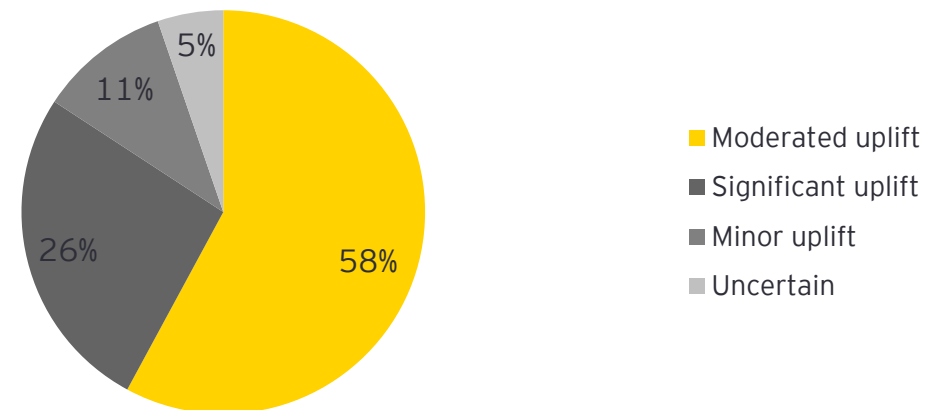
▶ 84% of CAEs believe that a moderate to significant uplift in capabilities will be required to demonstrate full compliance with the standard.

03

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

Responsibilities across the 3LoD



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

01

1

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

02

03

2

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

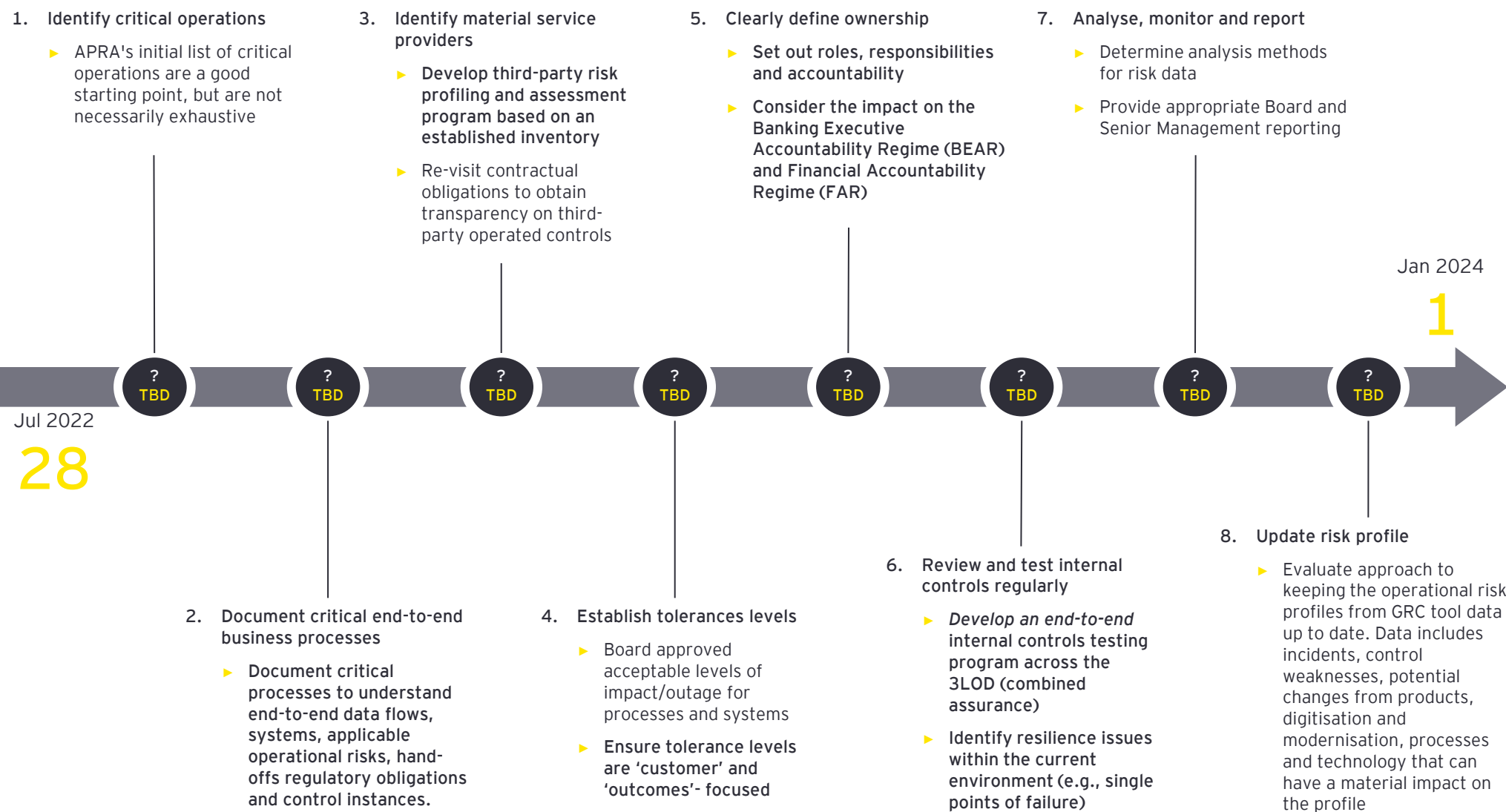
3

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.



01

02

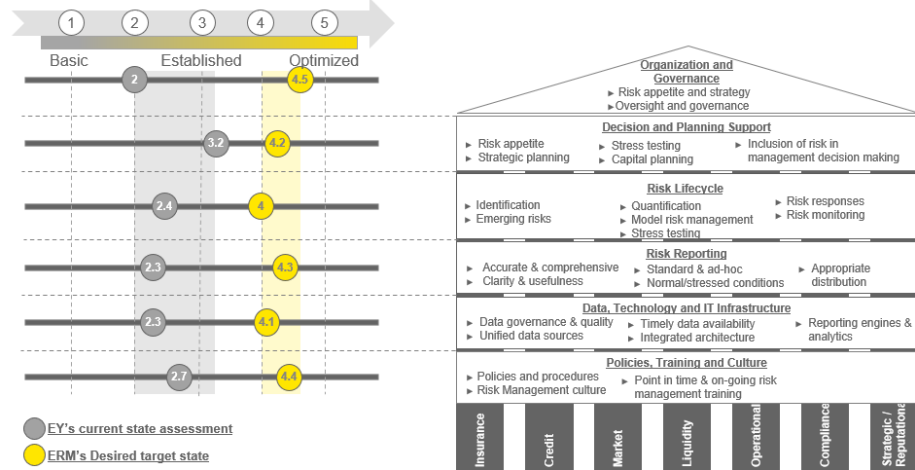
03

Operational risk framework diagnostic

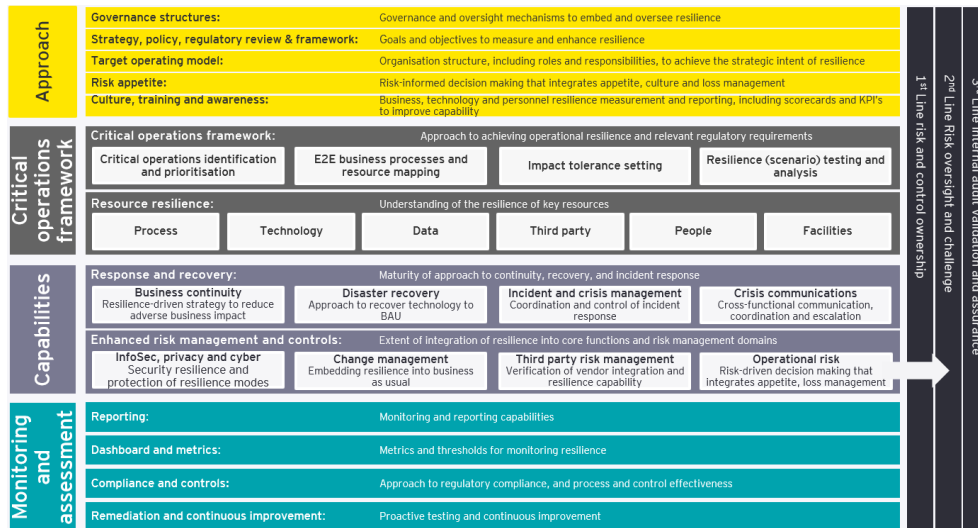
1. Perform a current state assessment of operational risk maturity against recent regulatory expectations and latest industry trends.
2. Compare the current state against minimum standards and any future defined target state.
3. For the gaps between the current state and target state, prioritise and 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 1	Level 2	Level 3	Level 4	Level 5	
	Basic	Established	Optimized	Rating (1-5)	Mean for ERM Component Subsection	Mean for ERM component
Organization and Governance	There is a basic operational risk framework document which has not been approved outside of second/third lines 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 ad-hoc basis. The framework is amended and applied differently in each business unit.	A formally documented operational risk management framework has been approved by Senior Management and Board. The framework aligns with the ERM framework. The framework is reviewed and updated on a regular basis. The framework is applied enterprise-wide and covers all material operations, including geographic, corporate, functional and material subsidiaries and joint ventures.	5		1.8
	The operational risk framework covers risk identification and assessment methods.	The operational risk framework covers most of RCSA, KRIs, Loss eventhous, misco, scenario analysis and loss tracking.	The operational risk framework covers all of RCSA, KRIs, Loss eventhous misco (internal indicators), scenario analysis, loss tracking, external loss, event and exposure, quantification and is up to date with all regulatory requirements. The framework ensures that the component work together consistently using same methods, wording, taxonomy, nomenclature etc. and aligns with ERM methodology, standards etc.	2		
	There is no Board-created enterprise level risk 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's operational risk committee reports. Committee meetings are held on an ad-hoc basis and without adequate times and resources to permit proper discussion and decision-making.	There exists a Board-created enterprise level risk committee for overseeing all risks, to which an operational risk committee reports. Committee meetings are held at appropriate frequency with adequate times and resources to permit productive discussion and decision-making.	2		
	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 (RCSA, KRIs, Loss Eventhous, Scenario analysis, 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 includes a combination of senior members with expertise in business activities, financial or risk management corporate and independent non-executive board members.	The Company's operational risk committee includes a combination of senior members with expertise in business activities, financial or risk management corporate and independent non-executive board members. Committee meetings are held at appropriate frequency with adequate times and resources to permit productive discussion and decision-making.	2		
	Risk Management and internal audit are the same function and are not independent (e.g. report to CFO).	There are three distinct lines of defense (1st line is the business, 2nd line is Risk Management, 3rd line is Internal Audit). Each line has its own mandate, responsibilities, and the third line is Internal Audit which address most risk topics. There is some overlap in responsibilities. There are adequate policies and procedures which identify respective responsibilities.	There are three distinct lines of defense around risk management which address all risk topics including those managed by material outsourced arrangements. There is no overlap in responsibilities, coordination of ERM process (including convergence of ORM, compliance, Legal, BCM, IT, Info Sec, Anticorruption) and an independent Internal Audit function. The three functions are coordinated, work together, have links overlap in responsibilities but are consistent terminology, assessment methodology and scaling for risk management.	2		
		Operational risk management functions exist in all of the business units and either have a direct or indirect reporting line to the CRO (controlled or decentralized). 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 units and either have a direct or indirect reporting line to the CRO (controlled or decentralized). Methodologies are consistent for all functions. Business functions still have sufficient independence to effectively challenge and report on BU risk management capabilities and report risk information timely to corporate function for consolidation and assessment.	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 unit/function, but do not effectively escalate issues and/or unacceptable risk exposure to Senior Management and Board.	There exists a robust and reliable escalation procedures which appropriately and timely escalate compliance issues, losses, breaches in the risk appetite limits to required to Senior Management, Board, or risk committees etc. Escalation points are consistent with the risk appetite and escalation limits.	2	2.4	
ERM	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 emerging 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.



Resilience risk framework diagnostic



01

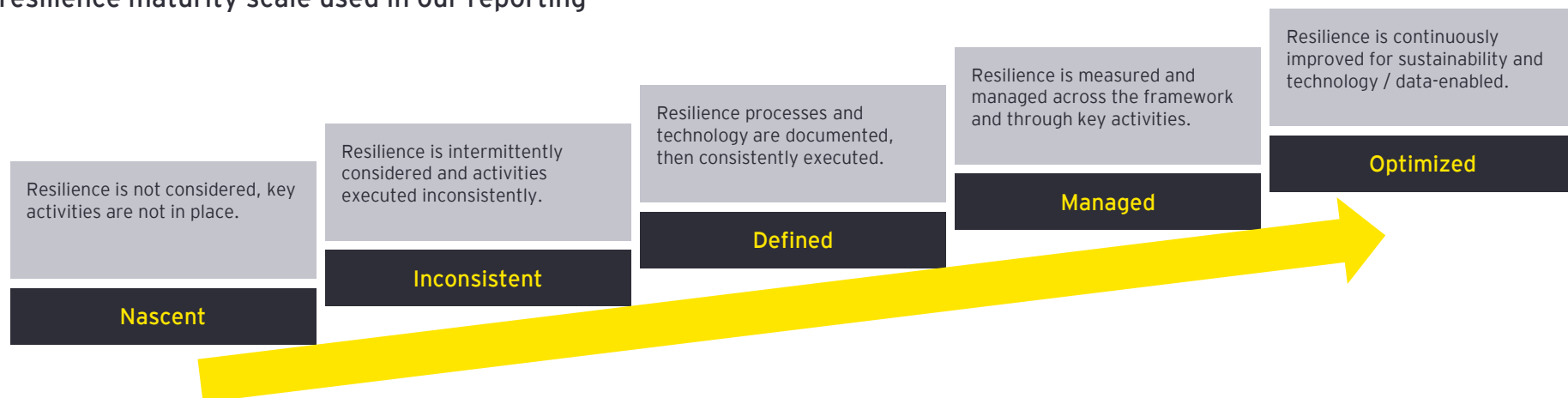
02

03

Maturity ratings against EY's operational resilience framework

Peer and industry benchmark

Our resilience maturity scale used in our reporting



EY | 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