CPS 230 – Operational Risk Management: Expectations and Compliance

IIA Financial Services Assurance Forum 2022

24 November 2022

EY

Building a better working world

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

Introduction and agenda

01

Key features

02

Key challenges

03

Actions to be taken

1 Key features

Why are regulators focused on operational risk and resilience?

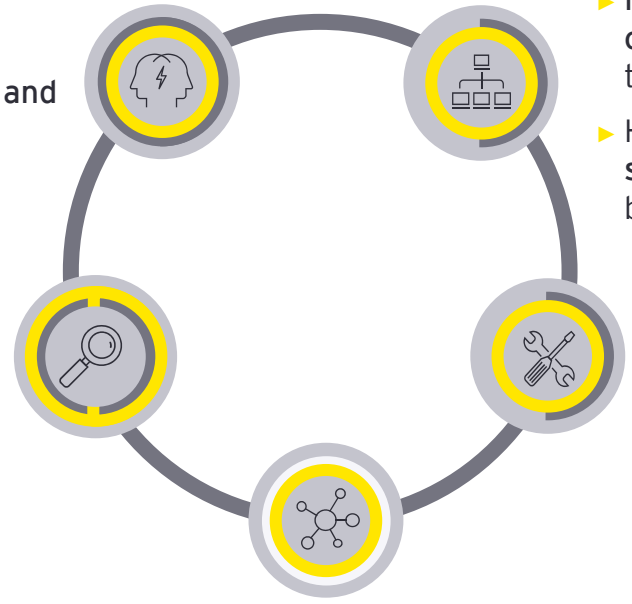
Operational risk and resilience have become a common focus area of regulators in the global markets.

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



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**

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"

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

Key changes

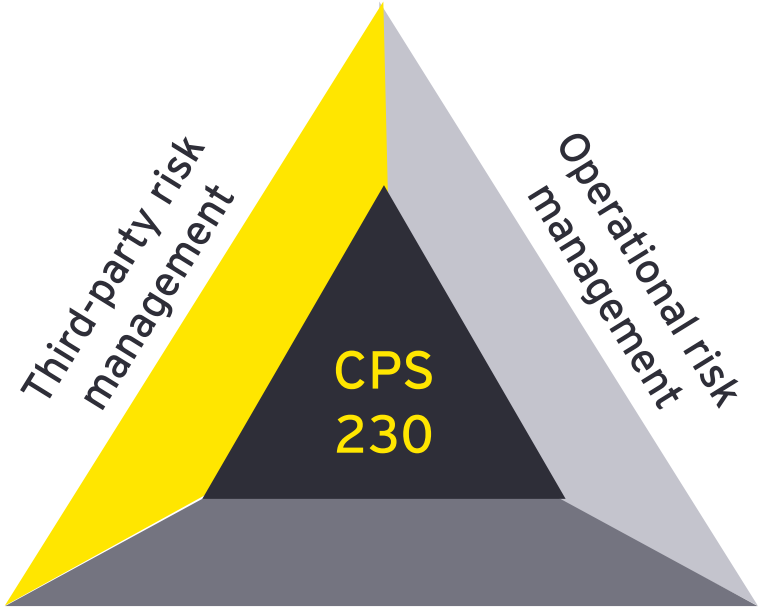
As global regulations start to align, we begin to see similarities with the UK operational resilience framework, the US Federal Reserve and the European Commission in the approach they are taking to Operational Resilience.

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



Operational risk

No previous operational risk standard

Operational risk only covered as part of CPS 220 requirements

No previously articulated requirements for controls

Business continuity planning

The focus is on critical operations and minimising disruptions to them

CPS 232 will be superseded by CPS 230

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.

Financial safety

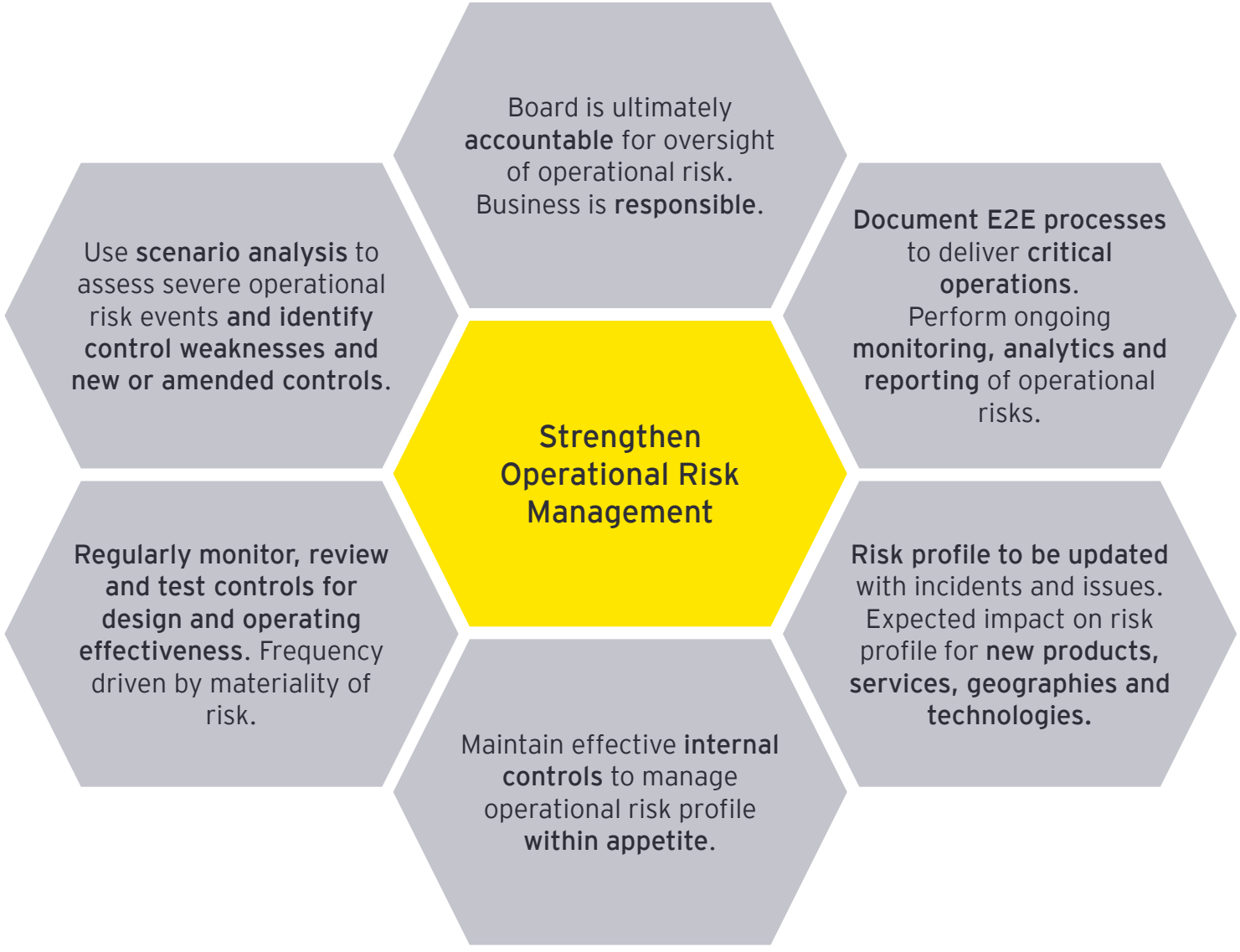
Financial system stability

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

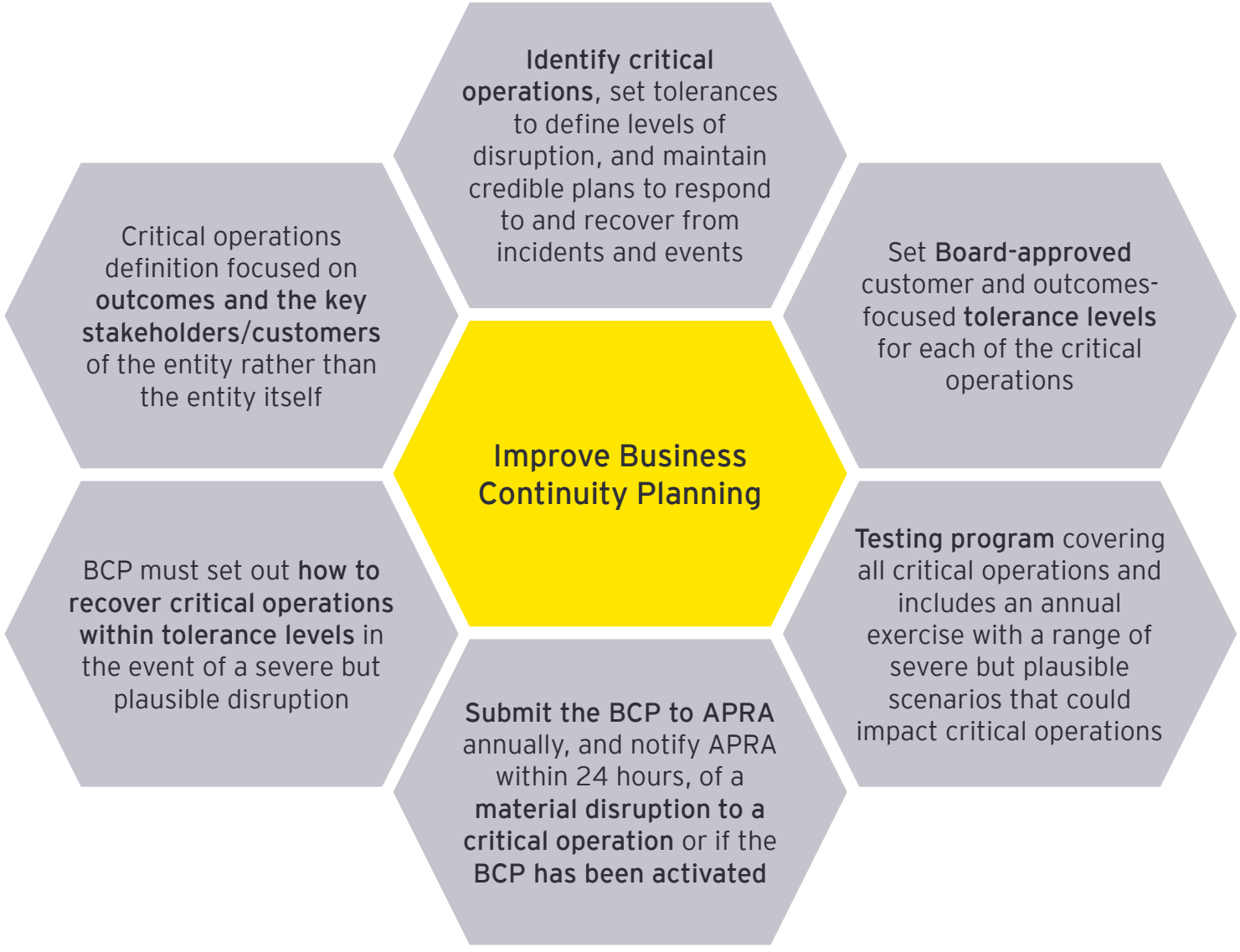
Critical operations, their processes, risks and controls have to be documented, monitored, analysed and reported. Control weaknesses and incidents should act as feeds to update risk profiles.

Customers and markets

What is APRA looking for?



What is APRA looking for?



What is APRA looking for?

2 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.

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
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.
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

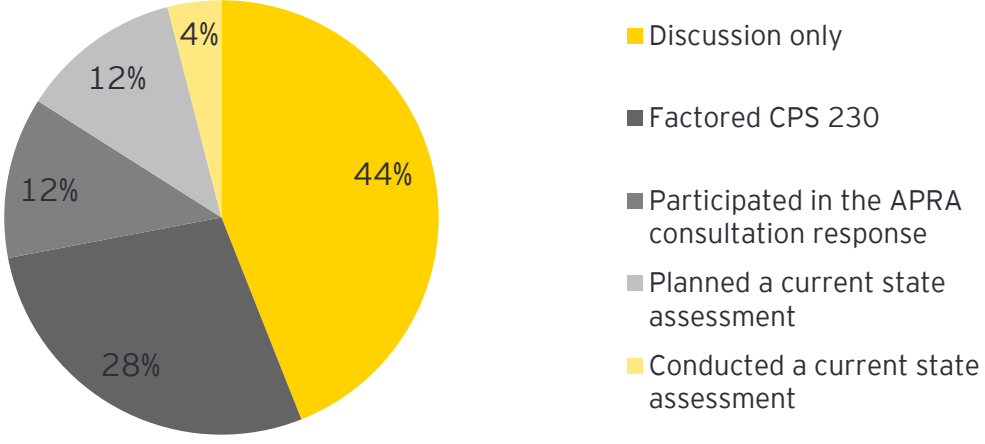
3 Actions to be taken

Insights from recent industry roundtable

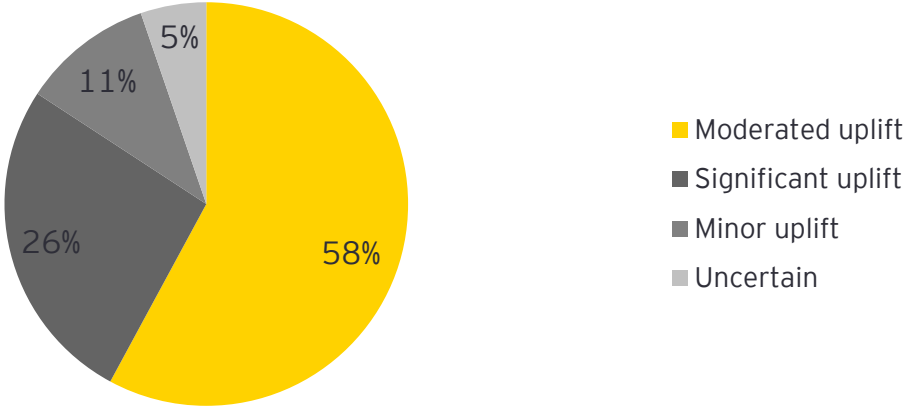
EY recently hosted an industry roundtable on CPS 230 attended by a cross section of CAEs from regulated entities in the Australian financial services sector. The roundtable gauged CAE views on key challenges and the likely response and role of internal audit functions.

- 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.
- 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?

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?

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

01

02

03

Responsibilities across the 3LoD

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

01

02

03

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

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.

Jul 2022
28

1. **Identify critical operations**
   - APRA's initial list of critical operations are a good starting point, but are not necessarily exhaustive

2. **Document critical end-to-end business processes**
   - **Document critical processes to understand end-to-end data flows, systems, applicable operational risks, hand-offs regulatory obligations and control instances.**

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 third-party operated controls

4. **Establish tolerances levels**
   - Board approved acceptable levels of impact/outage for processes and systems
   - **Ensure tolerance levels are 'customer' and 'outcomes'- focused**

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)**

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)**

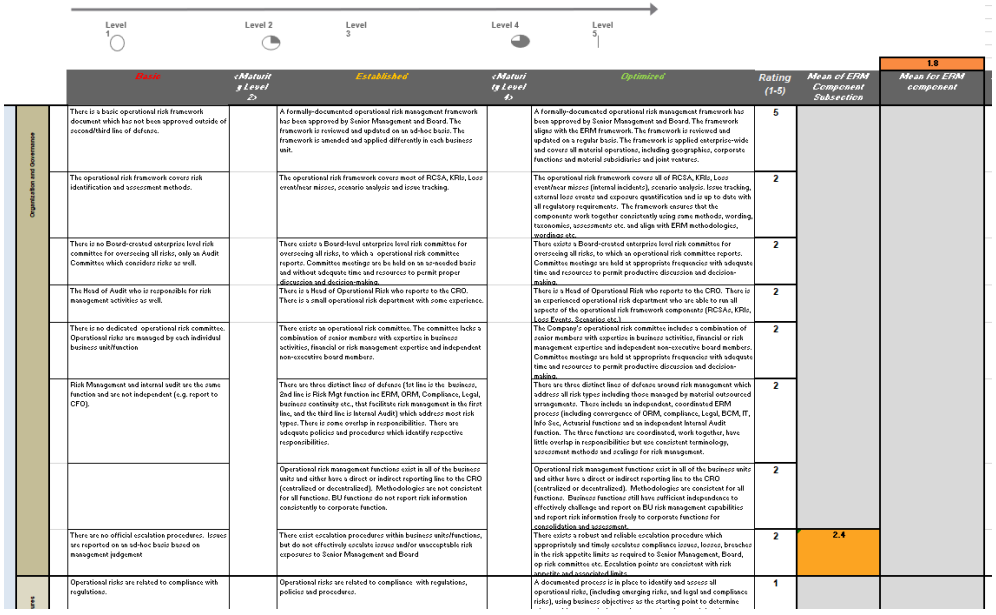
7. **Analyse, monitor and report**
   - Determine analysis methods for risk data
   - Provide appropriate Board and Senior Management reporting

8. **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

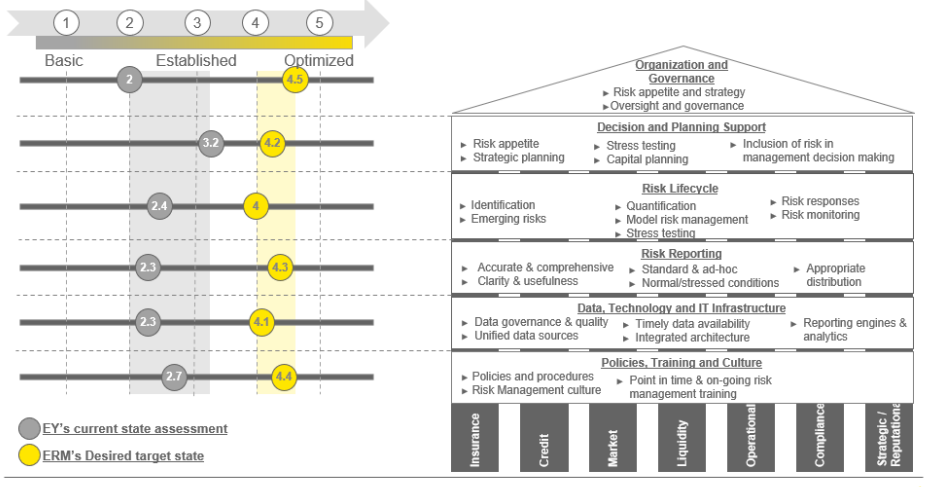
Jan 2024
1

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.

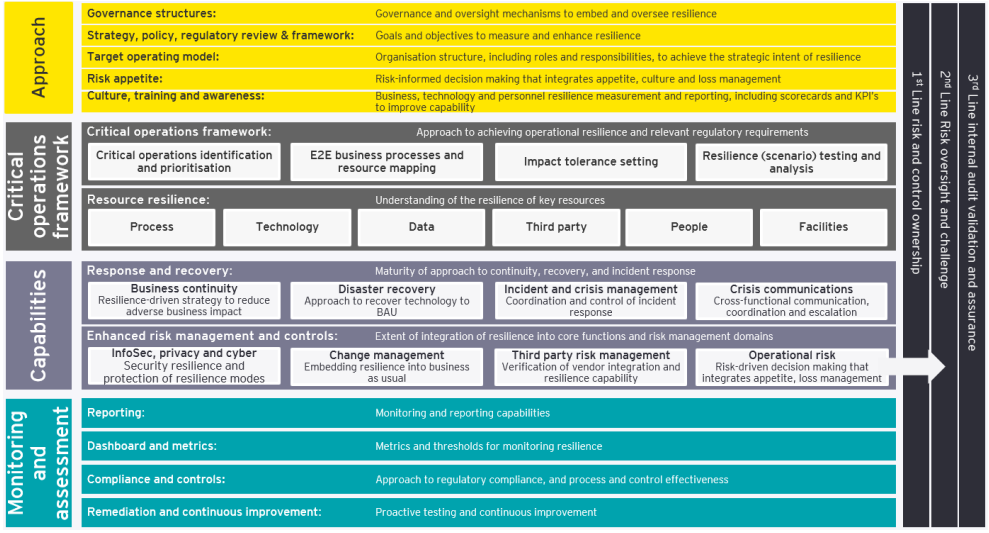


Based upon the observations made during the current state assessment, ERM program capabilities have been assessed against EY's ERM Framework maturity diagnostic tool and rated accordingly. The chart on the left *(below)* indicates EY's assessment of the current maturity rating and ERM program's desired 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.

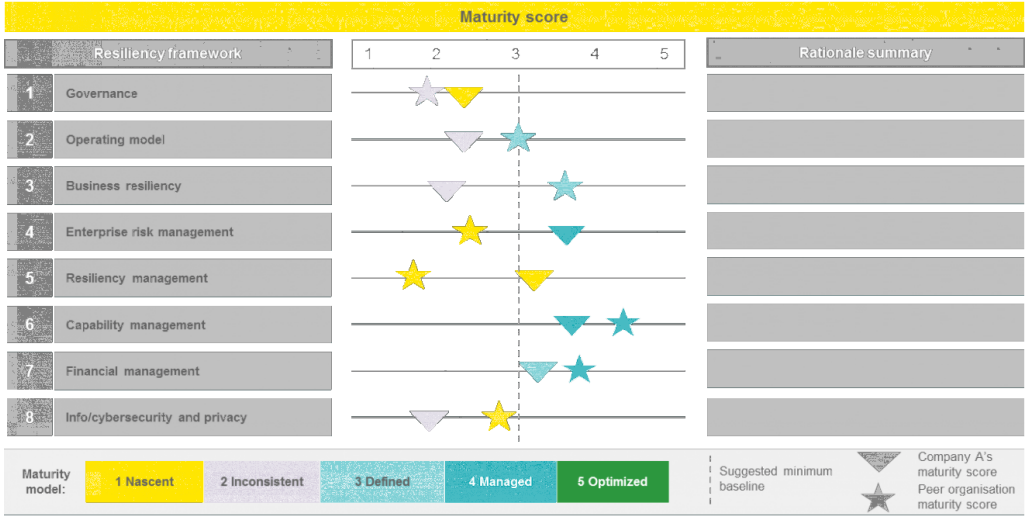


Source: EY Diagnostic Materials

Resilience risk framework diagnostic

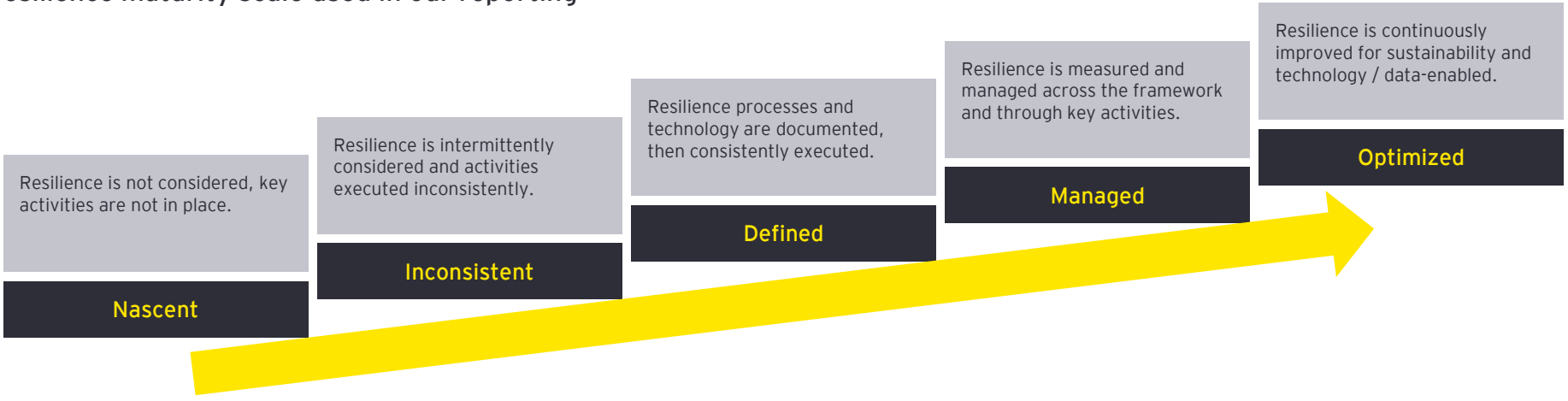


Maturity ratings against EY's operational resilience framework



Peer and industry benchmark

Our resilience maturity scale used in our reporting



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.

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.

ey.com