ANSARADA

1 Operational

2 Resilience

3 Outlook

4 Report

5 2024

6 Survey results and expert insights:
A comprehensive look at Operational
Resilience for the year ahead

Contents

01

Overview

About the report

We anonymously surveyed our Governance, Risk & Compliance (GRC) customer base and several professional risk communities to assess their current approach to, and outlook toward operational resilience. Survey respondents occupy roles across areas of risk management, legal & compliance, data governance, leadership and management, and consulting across industries.

We shared early survey findings with leading operational resilience authorities across Australia and the UK to include their views and their subject matter expertise in the final report. This report is the culmination of these survey results and expert opinions. In it, we address topics including the importance of resilience in today's risk landscape, where regulation is heading, how to anticipate and address future operational risks and challenges, how to implement a system for building resilience, and the role that technology can play in streamlining operational resilience management and compliance.

The survey results reveal a landscape with varying levels of preparedness, potential contradictions, and a need for more comprehensive frameworks. Addressing the identified challenges, such as resource constraints, knowledge gaps, and the use of legacy systems, is crucial for organisations to enhance their operational resilience.

Additionally, aligning the understanding of operational resilience with the self-assessed maturity level is vital for developing more effective strategies and frameworks. Regular assessments and a holistic, organisation-wide approach are key factors in building robust operational resilience.

We're incredibly thankful to all of our GRC experts for contributing their invaluable insights.

Kieran Seed, Head of Content, LexisNexis Regulatory Compliance

Heidi Richards, Independent Consultant and former APRA executive

Susan Bennett, Founder of InfoGovANZ and Principal of Sibenco Legal & Advisory

Simon Levy, CEO, Risk Management Institute of Australasia (RMIA)

Michael Rasmussen, GRC Analyst and Pundit, GRC 20/20

Rachel Riley Co-founder and Head of GRC, Ansarada

Return to contents

02

Intro

It’s time to embrace the era of constant change

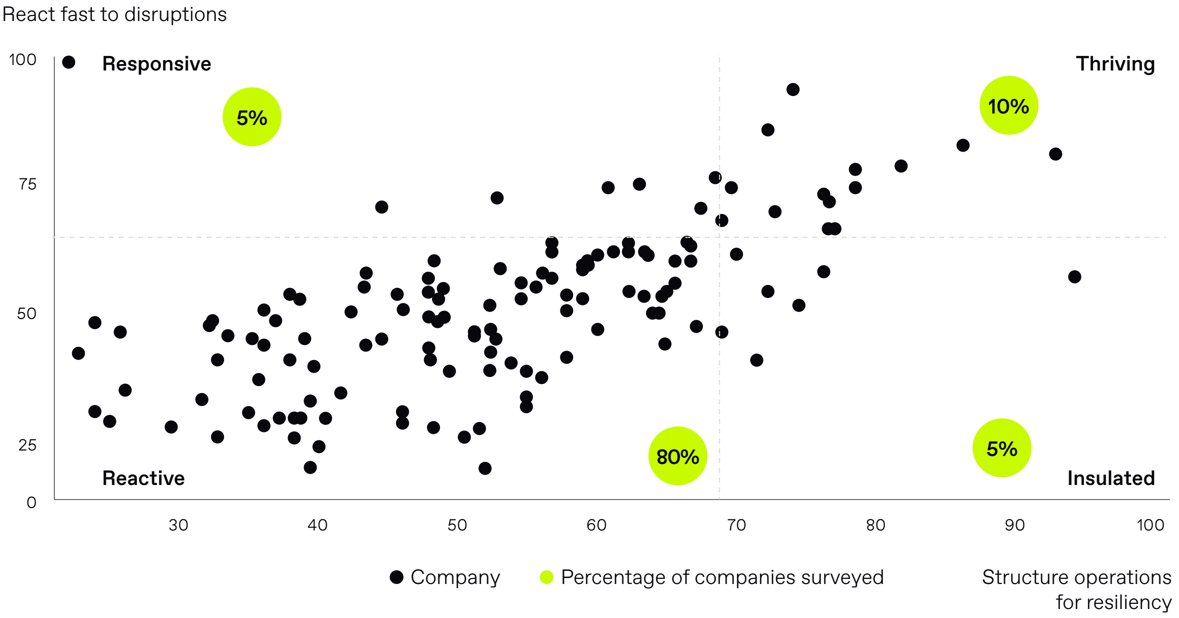
From multimillion-dollar data breaches to economic and geopolitical tensions and conflicts, today’s headlines are dominated by unpredictable events and upheaval. Disruptions are inevitable in our current risk environment. It’s not a case of ‘if’ disruption might happen, but ‘when’.

Most companies aren’t prepared for this inevitability. Data from BCG shows that only 10% of companies are ‘resilient and thriving’.

PwC’s recent 2023 Global Crisis and Resilience Survey found that an incredible 91% of organisations experienced at least one disruption over the last two years (excluding the pandemic), with 76% saying that their most serious disruption had a medium-to-high impact on operations, ‘disrupting critical business processes and services and causing downstream financial and reputational issues’. It’s no surprise, then, that 89% of respondents also said that resilience is one of their top strategic organisational priorities.

“Organisations are contending with external macro forces and internal business transformations, and it is against this backdrop that resilience has become one of the most vital strategic priorities in the corporate world,” said David Stainback, Co-leader of PwC’s Global Centre for Crisis and Resilience (PwC).

Only 10% of companies are truly resilient and thriving



The importance of operational resilience in today's risk landscape

Written by Kieran Seed, Head of Content, LexisNexis Regulatory Compliance - Global

Operational resilience is a critical focus for organisations across a wide range of industries. Australia, the United Kingdom, and New Zealand, among others, have introduced regulations requiring entities in critical infrastructure sectors – including energy, financial services, healthcare, transport and communications – to prioritise operational resilience. These regulations aim to ensure the uninterrupted availability and reliability of essential services, with non-compliance resulting in substantial penalties.

The healthcare industry, especially after the COVID-19 pandemic, has recognised the need for improved operational resilience. Healthcare providers are expected to have contingency plans in place to address demand surges and other operational challenges to ensure the continuous delivery of healthcare services.

Additionally, increasing reliance on third-party technologies, particularly across financial services, prompts organisations to consider the implications of such dependence on external partners. Industries such as technology and communications are proactively investing in disaster recovery and cybersecurity measures to ensure service continuity and minimise data breach risks when partnering with external technology providers.

Furthermore, boards and senior management teams are under mounting pressure to be accountable for their organisations' operational resilience. This increased accountability has elevated the importance of cultivating a resilient corporate culture. Directors and managers are now tasked with embedding operational resilience into the organisation's foundation, making it an integral part of strategic decision-making and risk management.

91%

of organisations experienced at least one disruption over the last two years (PwC)

These statistics highlight the importance of operational resilience for businesses. Companies must learn how to swiftly respond to disruption, accelerate digital transformation, and adapt operational practices in the face of such challenges by fully integrating all aspects of resilience into their Governance, Risk and Compliance (GRC) programs.

Over 76.6%

of organisations reported they have an operational resilience program in place or are building one (BCI)

03

Readiness

Return to contents

Assessing operational resilience maturity: How prepared are organisations?

Is there a common understanding/definition of operational resilience within your organisation?

50%	Yes
30.8%	No
19.2%	Unsure

Only half of all respondents have a common understanding or definition of operational resilience within their organisations, with 30.8% saying they do not, and 19.2% unsure.

Despite this uncertainty, only 26.9% of respondents rate their current operational resilience maturity as 'beginner' – over half (57.7%) rate themselves as 'emerging', and 15.4% rate themselves as advanced.

When it comes to implementing a formal operational resilience framework, the majority (53.8%) have one in the early stages of development, while 23.1% feel confident they already have a comprehensive framework in place. 19.2% of respondents have not implemented any formal framework, while a small percentage (3.8%) are unsure.

Return to contents

Has your organisation implemented a formal operational resilience framework?

53.8%	Yes, but it is still in the early stages of development
23.1%	Yes, we have a comprehensive framework in place
19.3%	No, we have not implemented a formal framework yet
3.8%	I'm unsure if we have implemented a formal framework

Does your organisation have a dedicated team responsible for overseeing operational resilience?

61.5%	No, operational resilience is managed by various teams across the organisation
36.4%	Yes, we have a dedicated team with clear responsibilities
3.8%	Not sure

Analysis of responses

Understanding versus maturity

These two results raise questions surrounding the understanding of operational resilience versus maturity. The majority of respondents consider themselves at an emerging level of maturity, which contradicts with only half indicating a common understanding of resilience. This raises questions about the alignment between perception and actual implementation.

Despite a sizeable portion (53.8%) having a framework in the early stages of development, the lack of a comprehensive framework for almost a fifth (19.2%) may impact the overall effectiveness of resilience efforts.

The contradiction between those with confidence in their frameworks and the overall lack of a common understanding is a point of concern.

Dedicated teams

Responsibility seems to be divided, with only 34.6% of respondents having a dedicated team for overseeing operational resilience. 61.5% say that operational resilience is managed by various teams across the organisation, while 3.8% are not sure.

With 61.5% stating that operational resilience is managed by various teams, and only 34.6% having a dedicated team, it suggests a potential lack of centralised oversight. This decentralised approach might hinder the efficiency and consistency of resilience efforts.

How would you rate your organisation's current operational resilience maturity?

Beginner	26.9%
Emerging	57.7%
Advanced	15.4%
Unsure	0%

> "
>
> Entities must build a new mindset about where their boundaries of responsibility sit. Perhaps the most significant change introduced by [APRA CPS230] is the requirement for an end-to-end view of operational risk, with a focus on critical operations, including those performed by third and fourth parties.
>
> Therese McCarthy Hockey, APRA
>
> "

04

Evolving regulatory environment

The expanding scope of operational resilience regulatory requirements

Financial services firms are particularly vulnerable to disruption because the potential operational risks they could face are significant, and could be enormously detrimental to our global economy and society. It's why the financial services industry operates in a highly regulated environment, and why recent operational resilience compliance mandates centre on these firms.

In today's landscape of fast-paced transformation, building operational resilience is crucial for all companies, regardless of size, industry, or revenue. Financial services may be the first to undergo operational resilience regulation, but they will by no means be the last.

A proactive approach to compliance is essential for navigating the web of mandates that vary across regions and avoiding costly payouts.

Globally, the Basel Principles for Operational Resilience build on existing operational risk principles 'to strengthen banks' ability to withstand operational risk-related events that could cause significant operational failures or wide-scale disruptions in financial markets.' Key regional standards and publications are outlined below:

> Collaboration between regulators, the government and industry is essential to develop and strengthen the regulatory framework and how organisations across financial services respond. So it's encouraging to see the Bank of England, PRA and FCA working closely to increase the resilience of the sector, while recognising the importance of supporting innovation.
>
> Dr Henry Balani, Global Head of Industry & Regulatory Affairs, Encompass Corporation

Region	Regulatory body	Standard or publication
United Kingdom	Financial Conduct Authority (FCA)	PS21/3 Building operational resilience standard
Australia	Australian Prudential Regulation Authority (APRA)	CPS 230 Operational Risk Management
Europe	European Council	Digital Operational Resilience Act (DORA)
Ireland	Central Bank of Ireland	Cross Industry Guidance on Operational Resilience
Hong Kong	Hong Kong Monetary Authority (HKMA)	OR-2 Supervisory Policy Manual (SPM)
United States	Federal Reserve System	Sound Practices to Strengthen Operational Resilience

The journey to an outcomes-approach to operational resilience

Written by Heidi Richards, Independent Consultant, former APRA executive

Operational resilience may be the latest buzzword that regulated financial institutions need to learn, but it's not a new concept. The emphasis on resilience to operational disruptions is just the flip side of the management of operational risks.

But the shift in language reflects an important evolution in regulatory philosophy – toward targeting good outcomes for companies and their customers, with accountability on the company to achieve those outcomes.

This shift in thinking results from decades of regulatory experience with enforcing more and more standards, checklists and processes, which have not resulted in any obvious reduction in operational failures among regulated financial institutions.

APRA's new standard CPS 230 is, in fact, largely a restatement and to some extent a streamlining of existing prudential requirements. What's new is the expectation of a more comprehensive and outcomes-focused approach to operational risk management across business units and across the traditional risk and compliance silos of business continuity planning, outsourcing and information security.

The outcomes focus is evident in the requirement that financial institutions set their own risk tolerances for resilience outcomes, and demonstrate that they are managing to those tolerances. To do this, the operational resilience mindset starts with the critical business processes and product/service operations, rather than risk management teams, processes and controls.

To understand the shift in mindset that is occurring, it's useful to consider how we got to this point.

Operational risk management as a discipline came into the regulatory gaze back in the 1990s after a series of rogue trader events at major global banks. At the same time, banking regulators from around the world were working on a new and (it was thought) more sophisticated regime for calculating capital requirements.

For a bank, capital on the balance sheet is critical to absorb unexpected financial losses and can help quantify and price risk. But capital comes with a significant cost to profitability, so, despite these benefits, banks have an incentive to minimise capital requirements.

A push by global banks for a more 'scientific' (and less costly) approach to model possible future losses for traditional bank credit and market risks led to the Basel II capital reforms in 2004. The thinking was the operational risks could also be managed in terms of financial loss impacts and risk-adjusted returns.

Continued by Heidi Richards

Under Basel II, banks would be accredited by their regulators to model regulatory capital requirements for operational risk, based on factors such as historical data, scenario-based potential losses and implementation of controls.

But unlike credit and market risk, quantitative modelling of operational risk capital was largely an experiment. There was no historical data, and little evidence that operational risk losses could be scientifically modelled or managed via capital incentives.

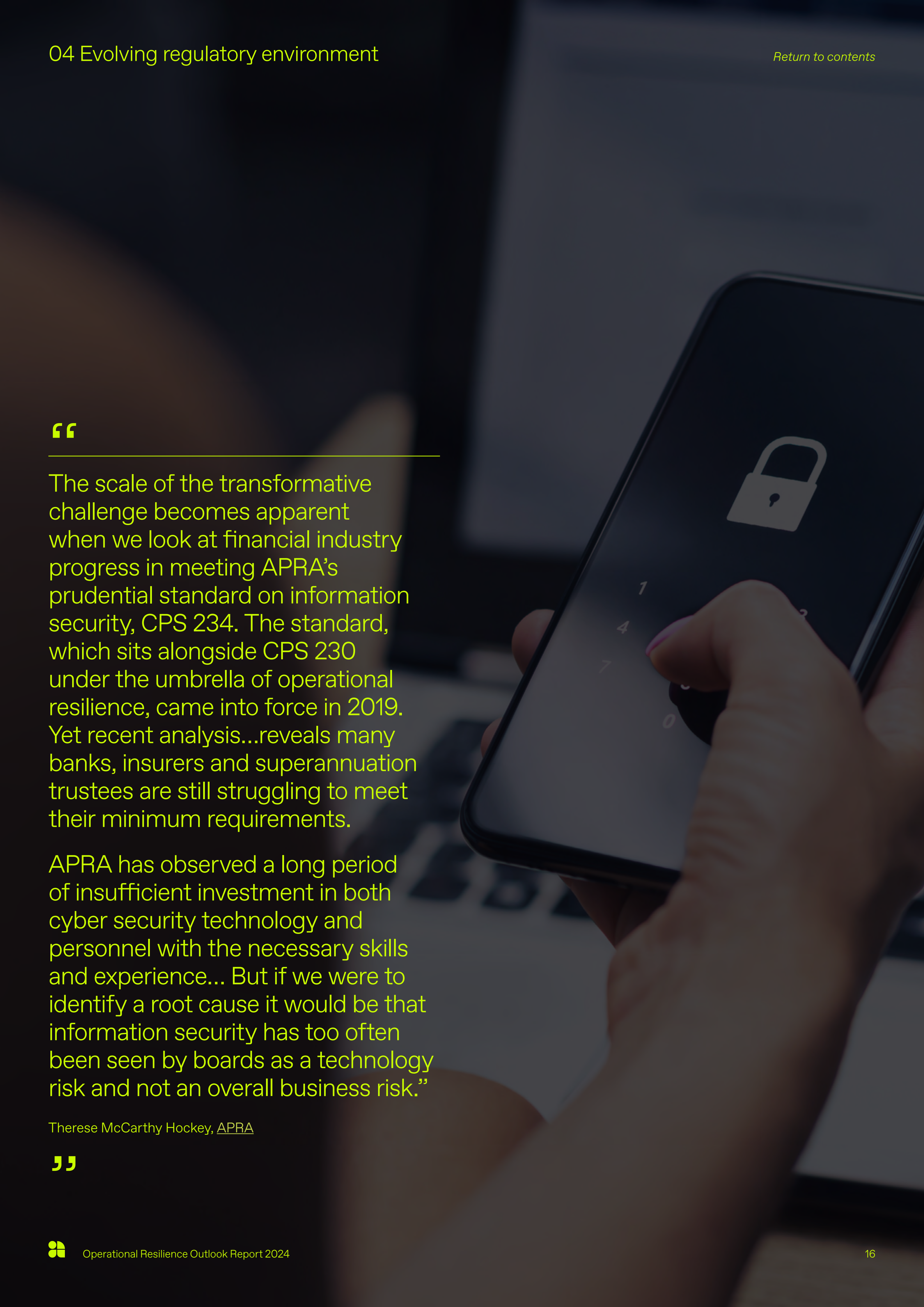
Despite this, the Basel II Advanced Modelling Approach was in place for 15 years at many global banks, including the major banks in Australia. At the same time, as technological change intensified and accelerated, information security, contingency and other technology-related risks grew in importance. Concerns emerged that the capital regime encouraged banks to focus on minimising a financial number, rather than minimising risk to them and their customers.

Ultimately, as part of the post-Global Financial Crisis regulatory reforms, operational risk capital modelling was largely abandoned. But this prompted some countries to push for a better approach – operational resilience.

Unlike capital or traditional risk silos, the concept of resilience is an opportunity to get business units and management involved. Modern tools to track and monitor resilience indicators, rather than backward-looking controls and risk maps, can be accessed by the whole organisation to provide transparency and accountability. Specialist skills may be required in areas like cybersecurity, but operational risk management will struggle to avoid being viewed as little more than a compliance exercise if it doesn't start and end with the business.

Regulatory change has increased by 500%

since the 2008 global financial crisis, heightening regulatory costs in the process (Ascent)



> "The scale of the transformative challenge becomes apparent when we look at financial industry progress in meeting APRA's prudential standard on information security, CPS 234. The standard, which sits alongside CPS 230 under the umbrella of operational resilience, came into force in 2019. Yet recent analysis...reveals many banks, insurers and superannuation trustees are still struggling to meet their minimum requirements.
>
> APRA has observed a long period of insufficient investment in both cyber security technology and personnel with the necessary skills and experience... But if we were to identify a root cause it would be that information security has too often been seen by boards as a technology risk and not an overall business risk."

Therese McCarthy Hockey, APRA

The real cost of non-compliance

The escalating volume and complexity of regulatory requirements is having a palpable impact on organisations. The range for non-compliance cost is between $2.20 million and $39.22 million. Total fines issued to financial firms between 2009 and 2020 approached $345 billion.

But the real cost of risk compliance chaos is not simply monetary; it extends to operational inefficiencies, reputational damage, and legal consequences.

The data shows that businesses are not spending enough on compliance. It becomes less about money and more about their focus areas. Proactively addressing cyber and digital risks in line with new operational resilience standards (as just one example) is a huge shift in focus for businesses.

As regulatory burdens continue to grow, organisations must recalibrate and strengthen their compliance strategies to ensure resilience in the face of constant change.

Since 2008, compliance-related operating costs have

increased by 60%

(Deloitte)

The cost of non-compliance is

2.7x higher

than the cost of compliance (Coforge)

> “
>
> Following a long period of consultation, feedback and drafting, new FCA rules on operational resilience finally came into force on March 31, 2022. Against the backdrop of the increasing risk posed by the cyber threat, the move comes not a moment too soon. However, it appeared to be getting precious little attention from industry experts, indicating that many firms may still be not prepared for the change.
>
> Evgeny Likhoded, Clausematch
>
> ”

Operational resilience just as crucial for non-regulated entities

Written by Kieran Seed, Head of Content, LexisNexis Regulatory Compliance - Global

Operational resilience is not exclusive to regulated entities. Non-regulated entities should prioritise operational resilience for several reasons:

Expanding scope of subject entities

In Australia and elsewhere, the scope of entities subject to operational resilience requirements has broadened under regulatory reforms. Non-regulated entities with inadequate regulatory change monitoring may unexpectedly find themselves under the purview of these regulations, necessitating proactive resilience measures.

Vendor expectations and supply chain risks

Regulated entities often extend their operational resilience expectations to their vendors and suppliers. Non-regulated entities within the supply chain of regulated entities must meet these requirements to maintain those business relationships.

Insurance and risk management

Demonstrating operational resilience can lead to lower insurance premiums. Organisations with comprehensive risk management plans demonstrate their readiness to mitigate and recover from disruptions, making them more attractive to insurers.

Business continuity and long-term viability

Operational resilience is not solely about recovering from crises; it also involves planning for long-term viability. Disruptions can result in financial losses that may threaten the survival of the business.

Return to contents

05

Mitigating key risks & challenges

Proactively dealing with critical risks

What are the primary challenges your organisation faces in maintaining operational resilience? (Tick all that apply)

57.7%	Lack of resources and budget constraints
50%	Inadequate communication and coordination between departments
50%	Competing priorities on other regulatory frameworks (e.g. ESG, 3rd party risk)
34.6%	Limited visibility and understanding of potential operational risks
30.8%	Building a business case for Directors and the Board
11.5%	Other • Lack of accountability and responsibility by risk owners • Ensuring all resilience requirements are captured. Combining IBS with business services that do not meet the FCA definition. • Size of company – 10 employees and competing priorities

Addressing primary challenges

When it comes to the primary challenges faced in maintaining operational resilience, ‘lack of resources and budget constraints’ is the top concern, cited by 57.7% of respondents. Half of all respondents also agreed that ‘inadequate communication and coordination between departments’ and ‘competing priorities on other regulatory frameworks’ are among their highest concerns.

‘Cybersecurity and data breaches’ are the primary operational risks being faced, according to 73.1% of respondents, followed by ‘regulatory changes and compliance failures’ (57.7%) and ‘third-party or supply chain disruptions’ (53.8%). 19.2% of respondents also specified ‘other’ key risks, including critical infrastructure, plane crashes, and the breakdown of controls or operational processes.

Looking forward over the next 5 years, it’s anticipated that ‘cybersecurity and data breaches’ will continue to pose the most significant operational risk, according to 64.5% of respondents. ‘Third party/ supply chain risk’ remains a key concern (57.7%), as does ‘the evolving regulatory environment’ (50%).

What are the primary operational risks that your organisation considers when assessing operational resilience? (Tick all that apply)

73.1%	Lack of resources and budget constraints
57.7%	Regulatory changes and compliance failures
53.8%	Third-party / supply chain disruptions
38.5%	Limited visibility and understanding of potential operational risks
19.2%	Other

- Critical Infrastructure
- Airplane crash
- Breakdown in controls or operational processes

“

> It’s one thing performing resilience audits to identify vulnerabilities, it’s another thing to get businesses to invest in the solutions. Competing programs don’t help if finances are an issue and the fact that risks may not have materialised make it challenging to flag it as urgent.

Survey respondent

”

Analysis of responses

Resource constraints

The top challenge, 'lack of resources and budget constraints' (57.7%), might hinder the effective implementation of operational resilience measures. This financial strain could impact the development of comprehensive frameworks and ongoing assessments. Resources are clearly having an impact on maturity levels and support with the combination of analysis showing distribution amongst teams and risks involved in a decentralised approach to resilience.

Operational risks

While there's a strong emphasis on cybersecurity (73.1%), other risks like regulatory changes and third-party disruptions are also significant. The challenge lies in balancing the attention given to different risk factors, especially with competing priorities.

Future risk anticipation

The alignment of current concerns with future expectations, particularly in the emphasis on cybersecurity (64.5%), indicates a recognition of persistent threats. However, a deeper analysis could explore whether organisations are adequately preparing for emerging risks like AI and climate events.

What areas do you believe will pose the most significant operational risk over the next 5 years? (Tick all that apply)

64.5%	Cybersecurity and data breaches
57.7%	Third party / supply chain risk
50%	The evolving regulatory environment
34.6%	Artificial intelligence / digital technologies
30.8%	Climate events and sustainability concerns
7.7%	Other

- The complexity of the VUCA world, creatitng unforeseen risks
- Economic environment and governance

Mitigating cyber, technology, third-party and ESG risks

Written by Susan Bennett, Founder, InfoGovANZ and Principal of Sibenco Legal & Advisory

The survey responses reveal the top three risks for organisations are cybersecurity and data breach, third-party supply chain risk, and complying with new and evolving regulations.

The fallout from a serious cybersecurity attack, regulatory compliance failure, ESG failures and loss of reputation, require organisations to implement effective systems and processes to improve identification and management of non-financial risks.

Key risks and challenges for organisations include:

- data and information governance as highlighted in high-profile data breaches with over-rentention of personal information; and

- accurate and timely data for emerging ESG requirements and measuring carbon footprint.

AI, technology and climate change were also identified by survey respondents as key risk areas for organisations in the next 5 years. This is hardly surprising given that Bill Gates declared in March 2023 that 'the Age of AI has begun' and we have seen the rapid take up of Generative AI along with the risks and problems from hallucinations to the use of confidential information and intellectual property ownership issues.

With the introduction of emerging regulations in both AI and ESG, organisations need to be on the front foot with developing appropriate internal systems to mitigate risks and comply with emerging domestic and international standards and regulations.

The key areas of risks identified by the survey responses, together with the complex operating environments for organisations, are drivers for boards and senior leadership teams to focus on building operational resilience to holistically govern and manage these risks.

Traditional GRC approaches and risk management frameworks need to evolve to meet the multifaceted risks and myriad of regulatory obligations. Holistic integrated governance and building operational resilience are mechanisms that can be implemented by organisations to meet the multifaceted challenges arising from the AI age, the increasing regulatory requirements and management of relentless cybersecurity challenges.

The World Economic Forum's Global Risks Report 2021 ranks 'extreme weather', 'cybersecurity failure', and 'IT infrastructure breakdown' among the top global risks.

Anticipating future operational risks

Written by Kieran Seed, Head of Content, LexisNexis Regulatory Compliance - Global

Future operational risks vary based on the organisation's circumstances, including its risk appetite, compliance maturity, location, industry, products, services, and vendor relationships.

Nonetheless, specific areas require focus:

Cybersecurity

Anticipated growth in the sophistication and frequency of cyberattacks increases operational risk, while the growing emphasis on cybersecurity reform imposes additional layers of compliance obligations across industries.

Third-party/supply chain risks

Organisations reliant on third parties face vulnerabilities if these parties fail to deliver, potentially impacting operations, the supply chain and financial stability.

Deloitte's 2023 Global Future of Cyber survey revealed that 91% of organisations had at least one cyber incident in the past year (up 3% from the previous year), with 56% of respondents suffering moderate to large consequences.

Artificial intelligence (AI)/digital technologies

Rapid adoption of AI and digital technologies has attracted significant regulatory scrutiny. The inherent complexities, ethical considerations, and potential risks associated with AI applications have prompted discussions about specialised, targeted regulations.

Climate events

Climate change effects can lead to more frequent and severe weather events, impacting physical infrastructure, supply chains and the availability of critical resources.

By prioritising operational resilience and staying informed about the risk landscape, organisations can ensure business continuity and long-term success. A compliance management system offers a structured approach to proactively identify, assess, and address regulatory and compliance risks, reducing the potential for costly penalties, liabilities, and reputational damage. This approach also allows for the continuous monitoring and adaptation of compliance practices, helping businesses stay resilient in the face of challenges.

06

The process of building & managing resilience

Legacy systems still prevail in operational resilience processes

When it comes to the process of managing operational resilience, the majority of respondents (42.3%) still use legacy systems like spreadsheets, Word documents and other manual applications, while 19.2% manage it as part of their GRC system, and 15.5% as part of their Business Continuity or Disaster Recovery system. Despite its strategic importance, only 7.7% of respondents use a dedicated solution for operational resilience.

In terms of frequency, over half of respondents (57.7%) conduct or plan to conduct resilience assessments regularly (at least once a year). Only 11.5% say this occurs 'rarely' (only when a significant event occurs), and 15.4% are unsure.

The most significant process challenge is cited as 'addressing the skills and knowledge gap' (65.4%), followed by 'conducting scenario testing' (53.8%).

To ensure ongoing monitoring and continuous improvement, half of all respondents planned to use a combination of tactics. Out of these tactics, 'regular risk assessments and scenario planning exercises' are the most common (23.1%), followed by 'regular audits and reviews of operational processes' (11.5%). Interestingly, despite the acknowledged skills and knowledge gap, 'employee training and awareness programs on operational resilience' fall last on this list (3.8%).

What systems do you currently use to manage your operational resilience?

42.3%	Word documents or other manual applications
19.2%	We manage it as part of our Governance, Risk & Compliance (GRC) system
15.4%	We manage it as part of our Business Continuity / Disaster Recovery system
15.4%	A combination of the above
7.7%	We use a dedicated solution for operational resilience
0%	Other

> Our approach has been to focus on our critical applications and then work backwards as to how to keep them operational in the event of a cyber/business interruption.
>
> Survey respondent

How does your organisation ensure (or plan to ensure) ongoing monitoring and continuous improvement of operational resilience?

53.8%	A combination of the below
23.1%	Regular risk assessments and scenario planning exercises
11.5%	Regular audits and reviews of operational processes
7.7%	Key performance indicators (KPIs) and metrics to track resilience levels
3.8%	Employee training and awareness programs on operational resilience
0%	Other

Analysis of responses

Tooling and systems

The prevalent use of legacy systems (42.3%) raises questions about the efficiency and scalability of current operational resilience processes. The low adoption (7.7%) of dedicated solutions might impede a more streamlined and integrated approach.

Frequency of assessments

The majority conducting assessments at least once a year (57.7%) is positive, showing a commitment to ongoing evaluation. However, the 15.4% unsure about their assessment frequency raises concerns about the consistency and rigour of resilience efforts.

Skills gap challenge

The identified skills and knowledge gap (65.4%) poses a critical hurdle. Understanding how organisations plan to address this gap is crucial for effective operational resilience. This flies in the face of the 3.8% (and lowest ranking) priority to improve operational resilience programs through employee training and awareness programs. This leaves a concerning potential lapse in addressing the skills and knowledge gap raised as a critical hurdle and priority.

What are your top challenges when it comes to managing the ongoing process of operational resilience?

65.4%	Addressing the skills and knowledge gap
53.8%	Conducting scenario testing
38.5%	Identifying and assessing supply chain risks
34.6%	Managing my operational risks
34.6%	Mapping the resources required to support important business services
23.1%	Reporting information back to the Board or regulators
19.2%	Managing my operational risks
0%	Other

How frequently does your organisation conduct or plan to conduct operational resilience assessments?

57.7%	Regularly, at least once a year
15.4%	Occasionally, every couple of years
11.5%	Rarely, only when a significant event occurs
15.4%	Not sure

Bridging the operational resilience skills & knowledge gap

Written by Simon Levy, CEO, RMIA

Our recent survey into the risk management profession found that many CEOs and business leaders are concerned about the growing skills and knowledge gap.

Here are some specific examples of how businesses can invest in raising standards and bridging the skills and knowledge gap:

- Provide training on risk management and resilience best practices. This training should be tailored to the organisation's and its employees' specific needs.
- Create opportunities for employees to develop their skills and knowledge through professional development programs, conferences, and other learning opportunities.
- Hire and retain qualified risk management and resilience professionals.
- Establish a culture of learning and continuous improvement.
- Businesses can build a strong foundation for organisational resilience by investing in or planning to address these areas.

How has the COVID-19 pandemic impacted your organisation's approach to operational resilience?

38.8%	It has highlighted the need for greater resilience and prompted improvements
34.6%	It has exposed vulnerabilities and weaknesses in our operational resilience
26.9%	It has not significantly affected our approach to operational resilience

07

Solutions for building resilience

Building and implementing operational resilience

Written by Susan Bennett, Founder, InfoGovANZ and Principal, Sibenco Legal & Advisory

Building and implementing operational resilience is achieved through a strategic and holistic governance by boards and the senior leadership team to systemically address risks, particularly those high risks areas which are managed across organisational silos and are interconnected including:

- The use of technology including AI – from procurement to implementation and ongoing management of technology systems.
- Data and information lifecycle management – from collection/generation, use/re-use, to disposal; and
- Regulatory compliance – ensuring data security and data minimisation requirements are met – including collecting only necessary personal data and disposal of data that is no longer needed by the organisation.
- Measuring carbon footprint of data and information being stored by the organisation and all the various cloud storage and physical archives.

In summary, a proactive and strategic focus on building operational resilience enables organisations to take a holistic approach to identify, measure and manage interconnected risks whether it be supply chain risk and information security or modern slavery concerns. By focusing on building organisational resilience, strategic priorities, actions and improvements in key risk areas can be more effectively monitored. This enables boards to improve overall corporate governance and organisational resilience while achieving overarching strategic objectives.

“

> Embedding an entirely new way of thinking about operational risk across an entire business operation will not be easy. Identifying compliance gaps and critical risk functions across third and fourth parties will not be quick. Upgrading systems and recruiting people with the requisite skills will come at a cost. But these enhancements are also not optional – not because it’s what APRA demands but because being protected from harm is an outcome that the community has come to reasonably expect.”

Therese McCarthy Hockey, APRA

”

Resilience from the unique perspective of CEO

Written by Simon Levy, CEO, RMIA

As CEO of the Risk Management Institute of Australia (RMIA), I have a unique perspective on the importance of organisational resilience. Organisational resilience is the ability of an organisation to anticipate, prepare for, respond to, and recover from disruptions. It is more important than ever for businesses of all sizes and industries, both regulated and non-regulated.

There are many reasons why organisational resilience is so essential now, including the increased frequency and severity of disruptions, the interconnectedness of the global economy, the impact of risk aggregation and the evolving regulatory landscape.

Businesses can build organisational resilience by identifying risks, developing a resilience plan, testing their program regularly, and creating a culture of resilience within their organisation.

Businesses can build organisational resilience by investing in the following:

- Identifying and assessing risks involves understanding the full range of potential disruptions that could impact the organisation and their likelihood and potential impact.
- Developing and implementing resilience plans should outline how the organisation will respond to and recover from disruptions, including steps to minimise disruption to operations, protect customers and employees, and maintain financial stability.
- Raising standards and bridging the skills and knowledge gap involves investing in training and education for employees at all levels to ensure they have the knowledge and skills they need to support the organisation's resilience efforts.

Investing in organisational resilience is essential for businesses to survive and thrive in today's uncertain world. By building strength, CEOs can protect their businesses from disruptions, create value for stakeholders, and contribute to the overall resilience of the economy.

08

Sentiment & future outlook

Return to contents

Organisations remain optimistic

Despite all the challenges, the vast majority of organisations (88%) are optimistic – albeit with some concerns. Only 12% feel underprepared to manage operational resilience in the year ahead. None of our survey respondents feel completely confident, indicating that there is some work to do.

How are you feeling about managing operational resilience for your organisation going into 2024?

88%	Optimistic, but with some concerns
12%	Underprepared
0%	Completely confident

Analysis of response

Optimism vs. underpreparedness

The high level of optimism (88%) despite the challenges suggests a positive outlook. However, the 12% expressing they are underprepared signals a potential disconnect between perception and reality. Other results indicate only half of all respondents have a common understanding or definition of operational resilience within their organisations, with 30.8% saying they do not, and 19.2% unsure. How can we be so confident in managing a disruption where a common understanding of resilience is unclear?

Understanding the specific concerns contributing to this underpreparedness is essential for targeted improvements.

No complete confidence

The absence of organisations feeling completely confident indicates a shared acknowledgment of ongoing work required. Analysing the specific concerns tied to this lack of complete confidence can guide targeted interventions for improvement.

The resilient organisation: Dynamic,

Disrupted & distributed challenges

Written by Michael Rasmussen, GRC Analyst and Pundit, GRC 20/20

Today's business has grown in complexity. This complexity, interwoven with the delicate balance of risks and objectives, demands organisations to adopt a strategic outlook towards operational resilience.

Historically, businesses operated in a simpler paradigm. However, today's enterprise has evolved due to increasing risks, stringent regulations, globalisation, multifaceted operations, competitive velocity, technological advancements, distributed relationships, and the deluge of business data. These impact businesses of all scales. Decision-makers at every level, from board members to executives and down to operational management, find synchronising business strategy, operations, and processes an immense challenge. This requires a 360° risk and resilience perspective. A deeper look at the survey data from Ansarada reiterates this perspective, indicating that 50% of organisations have a consistent definition and common understanding of operational resilience.

There's an unmistakable emphasis on resilience in today's business narrative. Resilience denotes an organisation's ability to recover from risk events swiftly. Increasingly, entities are merging operational risk management with business continuity management, transitioning towards an integrated risk and resilience management approach. The once standalone function of business continuity management is phasing out, with predictions indicating a surge toward integrated risk and resilience programs.

Resilience and the organisational hierarchy

Synchronising resilience with the ever-present business challenges proves daunting for executive and management professionals. The situation is exacerbated when continuity measures get relegated to departmental depths, are perceived purely from a compliance perspective, or are devoid of integration into broader risk management.

Return to contents

Continued by Michael Rasmussen

Today's organisations are:

Distributed

Even small-scale operations span the globe. Traditional business structures have evolved into complex networks of relationships and interactions.

Dynamic

Organisations adapt to evolving business operations, strategies, technologies, and risk landscapes. They must monitor diverse risk scenarios, including regulatory, geopolitical, economic, and operational ones, and the intersection of these.

Disrupted

The threat environment is complex and multifaceted. Managing copious amounts of structured and unstructured risk and resilience data across various systems disrupts the organisation, especially when agility is essential.

Accountable

There is increasing regulatory and legal pressure for resilience accountability at the top of the organisation. Today's leaders recognise the imperative to integrate risk management into business strategy and execution.

The challenge is being resilient in an organisation that is not static but constantly moving, evolving, and adapting. A change in one technology or process can trigger ripple effects throughout the organisation. Hence, a comprehensive understanding of an organisation's processes is vital to resilience.

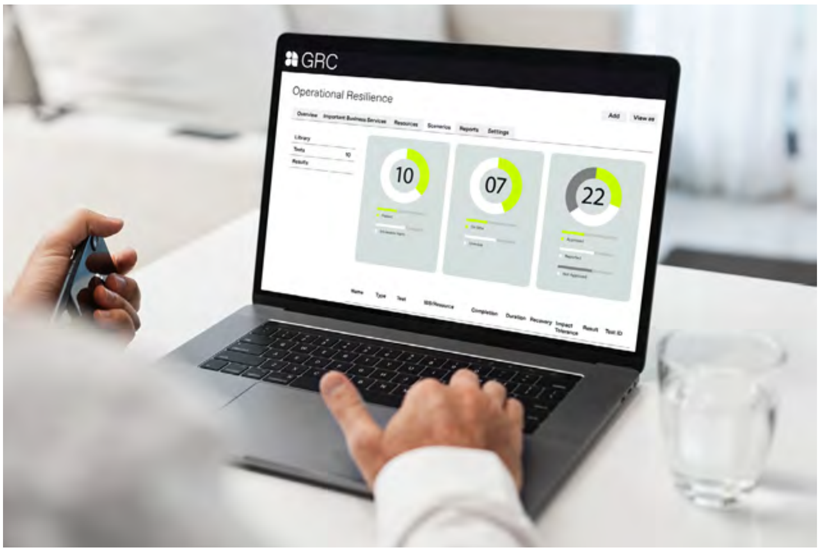
Data from the Ansarada survey underscores this interconnected business model, indicating that 53.8% of organisations have begun implementing an operational resilience framework, and 88% feel optimistic about their commitment to operational resilience going into 2024.

Businesses are merging their resilience programs into broader risk management frameworks. Some sectors even mandate this integration as a regulatory requirement. Such a merger ensures a comprehensive perspective on an organisation's objectives and processes, enhancing the synergy between risk management and business continuity.

Recognising that operational resilience is not merely an upgraded version of business continuity is crucial. Instead, it's a concerted effort that necessitates collaboration across risk management, resilience (formerly business continuity), and third-party risk management.

For businesses to thrive, they must thoroughly understand their operations, objectives, risks, and processes. The intricate relationship between business operations and risks emphasises the need for organisations to adopt an integrated approach to risk and resilience. Successful resilience strategies must blend strategy, processes, information, and technology seamlessly. This is an area where organisations have a lot to focus on with 42.3% stating they are trying to do this in manual processes with documents, spreadsheets, and emails in the Ansarada survey.

Moving to agile technology for risk and resilience management provides real-time awareness and enables continuous monitoring and quick adjustments to the evolving risk landscape, reflecting the organisation's current and desired states of resilience maturity.



Return to contents

Finding opportunity to thrive in the Resilience Revolution

Written by Rachel Riley, Co-founder and Head of GRC, Ansarada

Ongoing pandemic implications, market uncertainty, economic volatility, supply chain struggles, talent shortages, cybersecurity, geopolitical and climate risk are all concerning global trends for businesses to watch into 2024 and beyond.

It's no longer good enough to have a disaster recovery plan, ISO accreditation and yearly audits. Today, those checks are the absolute minimum baseline. Compliance standards do not consider the specifics, such as the organisation's business model, strategy and value proposition. Being merely compliance-driven does not guarantee an increase in resilience, nor does it enable the build of governance processes that are fit-for-purpose.

Operational resilience is more than just a regulatory requirement; it is an essential long-term strategy for progressing on wider company goals and increasing stakeholder interests such as sustainability and ESG.

As an organisation, you need to create an operational resilience framework taking a holistic view of your business, operations, finances, governance, regulation and compliance, information security, ESG impact and more. All core elements of the business need be 'operationally resilient' by design as organisations grapple with significant uncertainty and emerging risks.

Operational resilience allows an inside out view of risks. Firstly, what are our critical processes and what could impact these? This allows a holistic view of disruptive risks – not a siloed, archaic risk approach that looks at cyber, supply risks, panadamics etc, in silos. There is a growing concern that organisations do not understand or accurately estimate their level of unpreparedness. As we've seen in this survey, over half (57.7%) rate their operational resilience maturity as 'emerging', despite reporting that only half of them have a common understanding or definition of resilience. Organisations risk thinking that having a tested BCP and cyber plan with security reviews of third-party providers is good enough. It's not.

If you have not mapped out your critical processes and performed resilience testing against a range of plausible events, how can you possibly have confidence in your ability to withstand shocks?

If you can not answer questions such as 'what is your impact tolerance threshold and did testing remain in threshold?' for events against your critical processes, such as cyber, climate events, supply chain shocks and pandemic type disruptions, then you cannot be confident in your organisation's resilience. Ultimately, you are leaving your customers, the Board, the organisation and yourself at risk.

Return to contents

Continued by Rachel Riley

Use the opportunity to get your firm in order

The good news is that the scope of operational resilience provides a thorough lens across these issues and how organisations can, and will, perform when (not if) a critical event arises – whether it's a one-off event like a cyber breach or a sustained impact such as COVID-19.

More than that, viewing operational resilience holistically not only benefits the business, but also gets you ahead of the curve on what is becoming increasingly mandated regulation on ESG aspects. Global mandated regulations are increasing. Disclosures of this kind will soon be mandatory for business. Operational resilience, with its value chain analysis and climate resilience scenarios, lays the groundwork for compliance with emerging ESG legislation like ISSB S1, S2, and CSRD requirements.

Getting your operational resilience and overall GRC processes right is not only key to your success but is increasingly becoming a 'ticket to play' to stay on top of and address the ever-changing risk landscape and arguably, to exercise duty of care and diligence as these risks are now a core governance concern.

This quote from one respondent sums it up nicely:

> "If you're playing the course to 2030, operational resilience is a club you want to start packing today. Aim for a hole-in-one but if you land in a bunker, best to make sure you have more than a putter at your disposal."

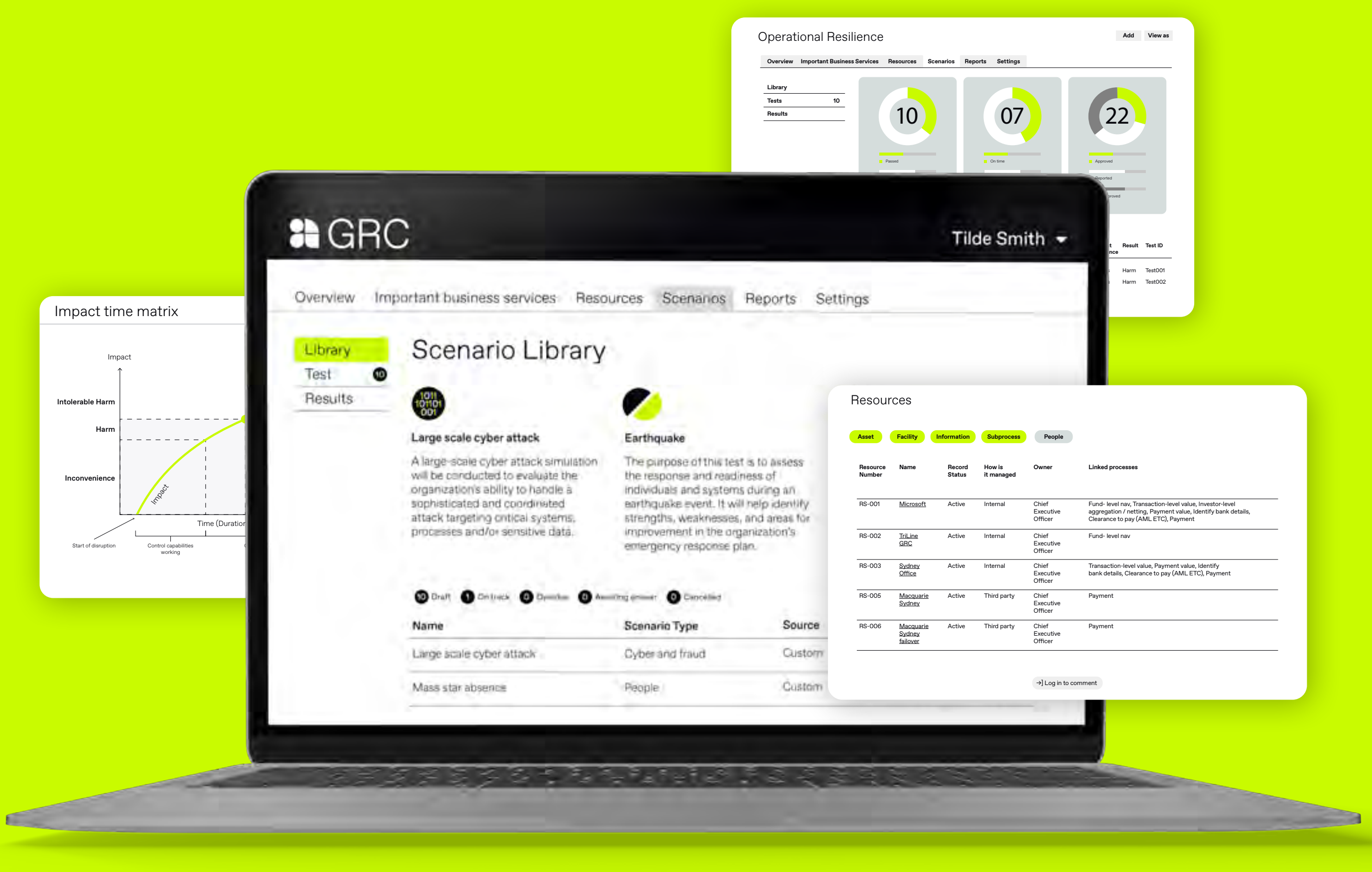
Beyond spreadsheets: A tech-driven approach to operational resilience

Ansarada has over 17 years' experience in information governance helping people get their businesses in order – from helping to transact over 1 trillion dollars in M&A deals and procurement on our platform, to technology enabling board meetings and GRC processes to run like clockwork.

Ansarada GRC provides a complete Governance, Risk and Compliance solution, integrating all facets of operational resilience. Our platform covers risk management, control assessment, event tracking, contract management, policy compliance, regulatory scanning and more. It not only maps critical processes, but also enhances visibility into third-party resources, supply chains, digital assets, and cybersecurity.

Our Operational Resilience solution allows you to manage current and future risk with purpose-built software, so you don't have to rely on spreadsheets or legacy systems. Connect data points across your entire organisation to bring order to chaos, eliminate risk silos and improve organisation-wide resilience.

Outsmart chaos and disruption with the leading Operational Resilience solution



Scenario Library

Large scale cyber attack

A large-scale cyber attack simulation will be conducted to evaluate the organization's ability to handle a sophisticated and coordinated attack targeting critical systems, processes and/or sensitive data.

Earthquake

The purpose of this test is to assess the response and readiness of individuals and systems during an earthquake event. It will help identify strengths, weaknesses, and areas for improvement in the organization's emergency response plan.

Name	Scenario Type	Source
Large scale cyber attack	Cyber and fraud	Custom
Mass star absence	People	Custom

Resource Number	Name	Record Status	How is it managed	Owner	Linked processes
RS-001	Microsoft	Active	Internal	Chief Executive Officer	Fund- level nav, Transaction-level value, Investor-level aggregation / netting, Payment value, Identify bank details, Clearance to pay (AML ETC), Payment
RS-002	TriLine GRC	Active	Internal	Chief Executive Officer	Fund- level nav
RS-003	Sydney Office	Active	Internal	Chief Executive Officer	Transaction-level value, Payment value, Identify bank details, Clearance to pay (AML ETC), Payment
RS-005	Macquarie Sydney	Active	Third party	Chief Executive Officer	Payment
RS-006	Macquarie Sydney failover	Active	Third party	Chief Executive Officer	Payment

Ansarada GRC delivers a world-first Operational Resilience solution to help you identify critical operations, set impact tolerances, test scenarios, and map resilience in a 360-degree dashboard view. Discover the simplest way to meet regulatory compliance standards for operational resilience with confidence, and build a resilient organisation.

Book a demo today

Bios

Kieran Seed

Head of Content, LexisNexis
Regulatory Compliance - Global

Kieran Seed is the Head of Content-Global for LexisNexis Regulatory Compliance, supervising and coordinating the development of complex compliance data sets locally and internationally. Kieran’s expertise lies at the nexus of compliance, law and content, to help organisations understand and monitor their compliance requirements in an accelerating and ever-changing regulatory landscape. Kieran’s team of subject matter experts manage a wide content set across the Pacific, UK and SEA, and also collaborate closely with content teams across the globe to bring the Regulatory Compliance solution to new markets and jurisdictions.

Heidi Richards

Independent Consultant,
former APRA executive

Heidi is a former senior regulator with 30 years experience leading policy and regulatory reforms at APRA, the Reserve Bank of Australia, the US Federal Reserve Board and US Treasury. Since retiring from the public service, Heidi provides guidance on regulatory strategy to banks and regulated financial institutions, fintechs, boards and CROs. Currently Heidi is focusing on scaling up risk and compliance functions, banking-as-a-service, operational resilience and open data. She loves to talk about improving how we design and implement regulation.

Susan Bennett

PhD, FGIA, CIPP/E, CIPT, Founder, InfoGovANZ and Principal, Sibenco Legal and Advisory

Susan is an independent corporate governance and privacy lawyer who works with Boards, senior executives and cross-functional multi-disciplinary teams on governance and data-driven technology transformation projects to minimise risks, comply with regulatory requirements and deliver on organisational objectives. Recognised for her global thought leadership in information governance, Susan brings deep corporate expertise to enable robust governance to be implemented to safely achieve the benefits derived from new technologies while simultaneously reducing risks through integrated and holistic governance in response to the growing legal and regulatory compliance challenges. These include privacy, cybersecurity, AML and emerging AI and ESG regulations, which require that technology systems be properly integrated and monitored, and that data is accurate, reliable for internal decision-making and external reporting, adequately protected and disposed of when no longer needed.

Susan's focus on driving best practice holistic governance solutions – aligning data, information, privacy and records with technology and regulatory compliance to achieve organisational goals, led her to found InfoGovANZ in 2016. The mission of InfoGovANZ is to break down the information silos among professionals to enable more connected thinking and innovation for information governance best practice and help drive more holistic solutions, particularly for data privacy and cybersecurity.

Simon Levy

CEO, Risk Management Institute of Australasia (RMIA)

Over twenty-plus years, Simon has led an impressive career as a Non-Executive Director, Chief Executive Officer, and Senior Risk Leader. His breadth of experience traverses several challenging and client-centric industry sectors, from professional services to health and aged care, retail, and manufacturing. Following three years of serving on the board of Australasia's leading professional risk body, the Risk Management Institution Australasia (RMIA), Simon was appointed its Chief Executive Officer. In this capacity, he has played a significant role in reshaping the future of the risk profession, strengthening its education and accreditation, and creating a collegiate network through which risk professionals can connect, communicate and learn to grow together.

Simon is enthusiastic about collaboration and promotion of the risk profession, providing an influential voice for the risk industry across its many professional engagements. A voice committed to enhancing the role of RMIA and the risk profession.

Michael Rasmussen

GRC Analyst and Pundit, GRC 20/20

Michael Rasmussen is an internationally recognized pundit on governance, risk management, and compliance (GRC)—with specific expertise on the topics of enterprise GRC, GRC technology, corporate compliance, and policy management. With 22+ years of experience, Michael helps organisations improve GRC processes, design and implement GRC architecture, and select technologies that are effective, efficient, and agile. He is a sought-after keynote speaker, author, and advisor and is noted as the "Father of GRC," being the first to define and model the GRC market in February 2002 while at Forrester.

Rachel Riley

Co-founder and Head of GRC, Ansarada

Rachel is the Co-Founder of ASX-listed tech company Ansarada Limited (ASX:AND) and currently serves as Head of GRC/ESG, shaping industry-leading products in governance, risk management, compliance, board management, and environmental, social, and governance (ESG). Her leadership empowers businesses with 360-degree visibility to navigate complex environments responsibly.

With over 12 years of experience at Ansarada, including executive roles like CFO, she brings extensive financial and operational management expertise, specializing in strategy, capital allocation, and fiscal project management. Rachel is a qualified Chartered Accountant with a Bachelor of Business and has spent over 7 years at KPMG in the Audit and Advisory division. Additionally, she serves as a Non-Executive Director and Chair of the Audit and Risk Committee at Interaction Disability Services, upholding the highest standards of information governance.

Return to contents

ANSARADA

ansarada.com