

OPERATIONAL RESILIENCE IS LEADING GRC TRANSFORMATION

Asia Pacific Market Research Report for ServiceNow

June 2023

This report was commissioned by ServiceNow, which asked Celent to design and execute a study on its behalf. The analysis and conclusions are Celent's alone, and ServiceNow had no editorial control over report contents.

INTRODUCTION

The recent failures of Silicon Valley Bank and First Republic Bank, the demise of Credit Suisse, and the spectre of additional bank failures were the latest in a series of high-profile threats to financial institutions' ability to operate uninterrupted. Over the last 25 years, we have seen the September 11 attacks in 2001, Global Financial Crisis in 2008, Flash Crash of 2010, Sovereign Debt Crisis in 2012, 2016 Bangladesh Bank heist, and the COVID-19 pandemic. Each severely threatened the viability of the financial services system.

In 2022, regulators around the world took action to instill more robust operational resilience to systemic risk across the financial services sector. While the regulations vary across geographies, they all bring together multiple aspects of operational risk into one framework—requiring an integrated risk management approach that designates across the enterprise what the critical business services are and specifies how they will be addressed in the face of systemic failure.

With most regulators requiring enhanced processes and systems to be in place by 2025, FIs have an urgent and critical need for help in transforming their risk capabilities. Many FIs are finding that, to respond to regulatory requirements, they need a higher level of coordination across the firm. They need to improve both the enterprise-level visibility into risk and compliance activities as well as their ability to coordinate responses at the enterprise-level.

This report looks more closely at these dynamics across Asia Pacific, covering:

- Existing and pending regulations driving change
- Operational requirements FIs will have to meet
- Heightened expectations being thrust on bank CROs
- Different levels of Governance, Risk, and Compliance (GRC) maturity across banks
- Different approaches FIs are taking to GRC systems

KEY FINDINGS

Operational Resilience

- Operational resilience (“OR”) regulations are being issued by financial regulators globally
- These regulations have 80–85% overlap across the world, simplifying adherence for multi-jurisdictional institutions
- Australia, Hong Kong, Singapore, India, and Japan have all issued new regulations or guidance. Australia and Hong Kong banks have the strongest imperative to transform to meet new regulatory requirements due to their breadth and the near-term requirement to implement
- Operational resilience regulation requires FIs to operationally manage risk in a coordinated way across the organisation

CRO Priorities and Preparedness

- Operational resilience was the 5th most listed priority in a 2023 survey of Chief Risk Officer (CRO) priorities
- 74% of bank CROs are in the process of implementing changes necessary to comply with OR regulation:
 - 49% of banks are still figuring out how to respond
 - 26% of banks feel they have already made all the necessary changes

GRC Maturity and Transformation

- Most of the FIs we interviewed were able to compile an integrated view of risk, but none were in a position to manage risk in a coordinated way across the enterprise level
- The financial institutions we interviewed across Asia Pacific were currently using an LoB-led or enterprise-led approach to integrating risk—neither of which facilitates managing risk in a coordinated way across the organisation

AGENDA

1

Operational Resilience

Regulations driving change

- In 2022, regulators around the world took action to instill more robust operational resilience to systemic risk across the financial services sector
- While regulations vary across geos, all bring together multiple aspects of operational risk into one framework
- These regulations require FIs to update risk processes and systems in order to comply. Most regulators require compliance by 2025
- To comply with operational resilience regulation, FIs must build an integrated risk management approach at the enterprise level

2

CRO Priorities

Increased demands on CROs

- Operational resilience is a priority for boards and FI CEOs, but they are looking to Chief Risk Officers to execute change
- 76% of banks are still implementing changes, and 45% are still figuring out how to respond
- Governance, Risk, and Compliance systems are at the heart of building enterprise-level integration
- Many FI CROs are struggling to integrate the myriad GRC systems that exist across their organisations

3

GRC Transformation

Increased demands on GRC systems

- FIs' enterprise-level GRC processes and systems are at different levels of maturity
- All but the most mature are transforming GRC capabilities to:
 - Integrate both divisional silos and operational risk functions
 - Use automation and AI to reduce cost of compliance
 - Ground additional capabilities into FI operations (1st line of defence)
- We see FIs taking four different approaches to GRC transformation

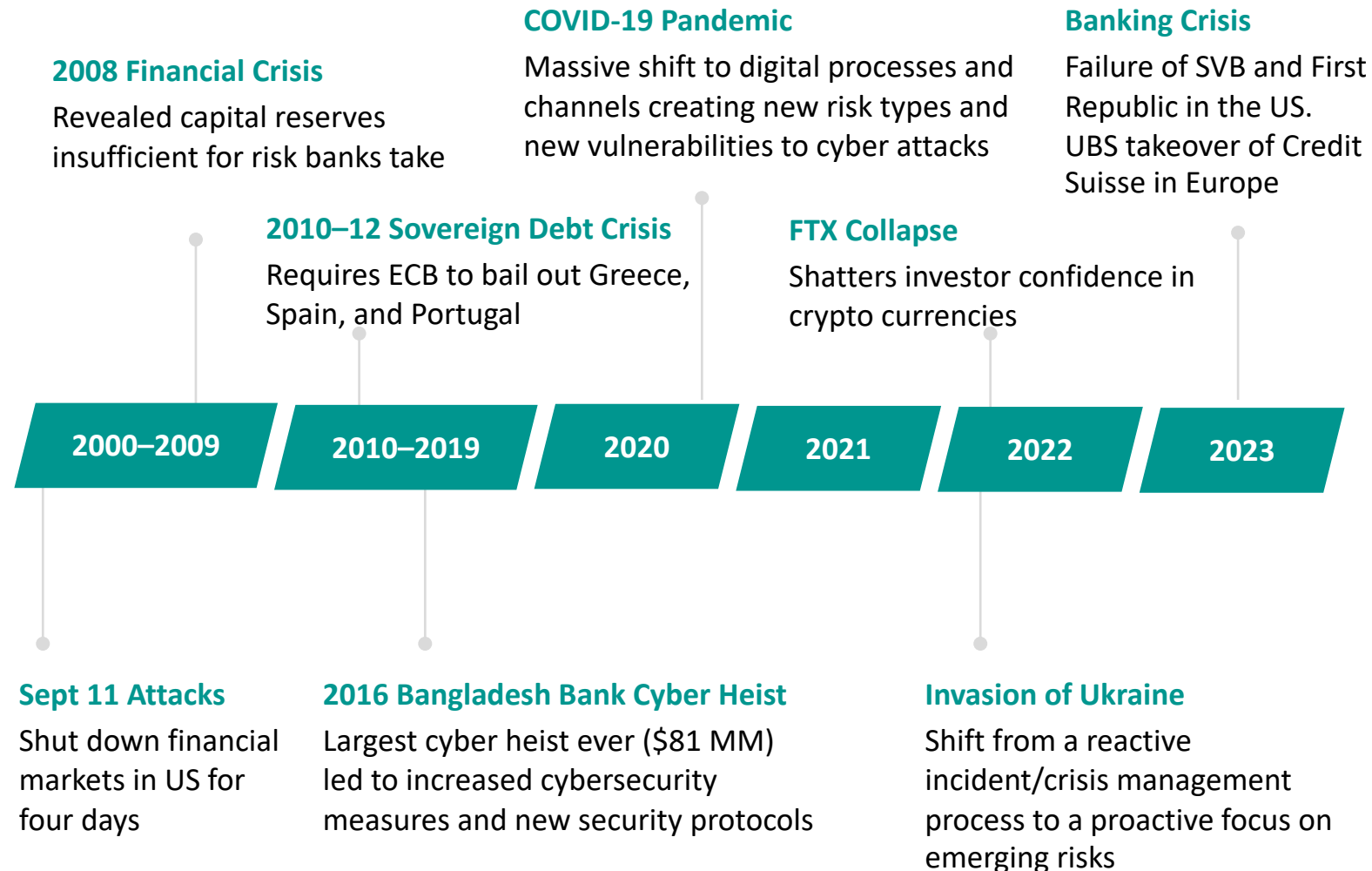
1 OPERATIONAL RESILIENCE

KEY POINTS

- Operational resilience combines operational risk management, IT risk management, business continuity planning, and third party vendor management
- Regulators around the world are issuing new requirements to increase financial institutions' operational resilience
- These regulations have 80–85% overlap across the world
- UK and EU are setting the pace for operational resilience
- Asian countries are consulting pacesetters' regulations as they issue regulations of their own
- Operational resilience regulation is driving GRC transformation

WHY FOCUS ON OPERATIONAL RESILIENCE?

Reaction to a series of high-profile threats in last 20 years



1. 80–85% estimate from KPMG International gap analysis
Source: [KPMG International](#), Celent analysis

Operational Resilience Regulation

View that post-crisis reforms had not fully addressed threats has led to a spate of regulation across the globe regarding OR
80–85% of content is similar across all geos¹

Most regulation contains these requirements

- Identify **critical operations** and set tolerance levels for each
- Develop **alternative delivery strategies** for each critical operation
- Run **scenario testing** on severe but plausible situations
- Notify regulators of any material **risk incidents**
- Actively manage **critical third parties**

WHAT IS OPERATIONAL RESILIENCE?

Five key components

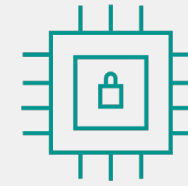
CRITICAL BUSINESS SERVICES

Identify critical business services and alternative delivery strategies for them. Define impact tolerances for severe but plausible scenarios.



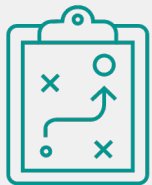
INTEGRATED EXERCISES AND TESTING

(Stress) testing of process and technology resilience to drive continuous improvement.



THIRD PARTY RISK MANAGEMENT

Extension of regulatory oversight to critical third and fourth parties, with particular focus on technology providers.



BOARD ACCOUNTABILITY

Board is required to review and approve operational resilience plans and procedures. Board members must develop and maintain understanding of ICT risk.



INCIDENT AND CRISIS MANAGEMENT

Activation of resilience strategies and notification of regulators when an incident occurs.



MAJOR OPERATIONAL RESILIENCE REGULATIONS IN EFFECT

Regulation in the UK and EU has provided a baseline that many regulators around the world have followed¹

UNITED KINGDOM



Operational Resilience Framework

Regulators: Bank of England, PRA, FCA²
Enacted: March 2022
Effective: March 2023
Objective: Protect financial system from systemic failure

Key Operating Requirements

- Identify important business services
- Set an “impact tolerance” for each service
- Run scenario testing to ensure ability to operate severe but plausible scenarios

Notes

- First to put operational resilience regime into effect
- Broader than DORA, which focuses on ICT³
- UK banks given one-year implementation period

EUROPEAN UNION



Digital Operational Resilience Act (DORA)

Regulators: European Council
Enacted: November 2022
Effective: January 2025
Objective: Bring guidance and stricter oversight on how ICT⁴ risks are managed

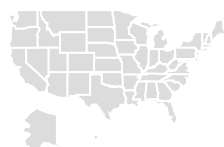
Key Operating Requirements

- Institute integrated ICT risk management framework
- Report ICT incidents – early warning indicators
- Conduct wide variety of tests of resilience
- Actively manage third party risk
- Share information with peers on cyber threats

Notes

- Adopted by EU in November 22, now being written into law by each EU member state

UNITED STATES



Sound Practices to Strengthen Operational Resilience

Regulators: Federal Reserve, OCC, and FDIC³
Effective: November 2020
Objective: Consolidate existing guidance on practices banks expected to have in place

Key Operating Requirements

- Identify important business services and set impact tolerances for disruption
- Immediately notify regulators of any “material” cybersecurity incidents
- Run scenario testing to ensure ability to operate severe but plausible scenarios

Notes






- Only focused on reducing systemic risk to FIs – not on levels of harm to clients

1. The Basel Committee’s Principles of Operational Resilience published in 2021 provided a framework with which regulators want to be compatible.

2. Prudential Regulatory Authority (PRA), Financial Conduct Authority (FCA). 3. Federal Reserve Board, Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC); 4. Information and Communication Technology
Source: Regulatory authority publications, legal analyses, Celent analysis

OPERATIONAL RESILIENCE REGULATION IN ASIA PACIFIC – OVERVIEW

Australian and Hong Kong financial institutions have the strongest imperative to transform to meet new regulatory requirements

	Australia	CPS 230: Operational Risk Management	Australian Prudential Regulation Authority (APRA)	<ul style="list-style-type: none"> Guidance on all five components of operational resilience In July 2022 APRA issued draft guidance. Now taking comments and will finalise by mid 2023 APRA just pushed back the date banks need to implement from January 2024 to 1 January 2025
	Hong Kong	Supervisory Policy Manual (SPM) module OR-2 on Operational Resilience	Hong Kong Monetary Authority (HKMA)	<ul style="list-style-type: none"> Guidance includes all five components Guidance issued May 2022 Banks need to develop operational resilience framework by 31 May 2023 and implement framework by May 2026
	Singapore	Business Continuity Management Guidelines	Money Authority of Singapore (MAS)	<ul style="list-style-type: none"> MAS issued two papers in summer of 2022 First gives guidance on 4 of 5 operational resilience areas – much in line with Dora and UK framework. Banks have one year from June 2022 to implement
		Information Paper on Management of Third Party Arrangements	Money Authority of Singapore (MAS)	<ul style="list-style-type: none"> Issued a second paper in June 2022 to cover third party risk management. Banks have one year from August 2022 to implement
	Japan	Ensuring Operational Resilience Discussion Paper	Japan Financial Services Authority (JFSA)	<ul style="list-style-type: none"> JFSA paper presents a framework based on international trends Will use the paper to promote dialogue with FIs, but will not formally apply individual requirements Paper released 16 December 2022
	India	Master Direction on IT Outsourcing	Reserve Bank of India	<ul style="list-style-type: none"> Issued June 2022 Go into effect 1 October 2023

Note: See Appendix for additional detail on regulation in each jurisdiction

Source: Celent analysis

OPERATIONAL RESILIENCE COMPLIANCE REQUIRES INTEGRATED RISK MANAGEMENT

Operational resilience regulation requires FIs to operationally manage risk in a coordinated way across the organisation.

Specifically to:

- Designate and agree across the enterprise what business services are critical and set an impact tolerance for each
- Map end-to-end dependencies for each service, including third parties
- Establish a comprehensive testing regimen of process and technology resilience to ensure that expected disruptions are within tolerance levels
- Ensure approach to third party risk management in accordance with key principles issued by the regulators
- Enable board and senior management need to attest that the FI is “operationally resilient”

Areas requiring risk management at the enterprise level



2

CHIEF RISK OFFICER PRIORITIES

KEY POINTS

- Operational resilience is a Chief Risk Officer (CRO) and board priority
- Banks are adopting an Integrated approach to risk management because it is a better way to protect the bank
- Regulatory pressures make this change urgent
- Improving operational resilience requires changing processes and systems
- An effective GRC system can allay regulators' top concerns

CHIEF RISK OFFICER AGENDA 2023

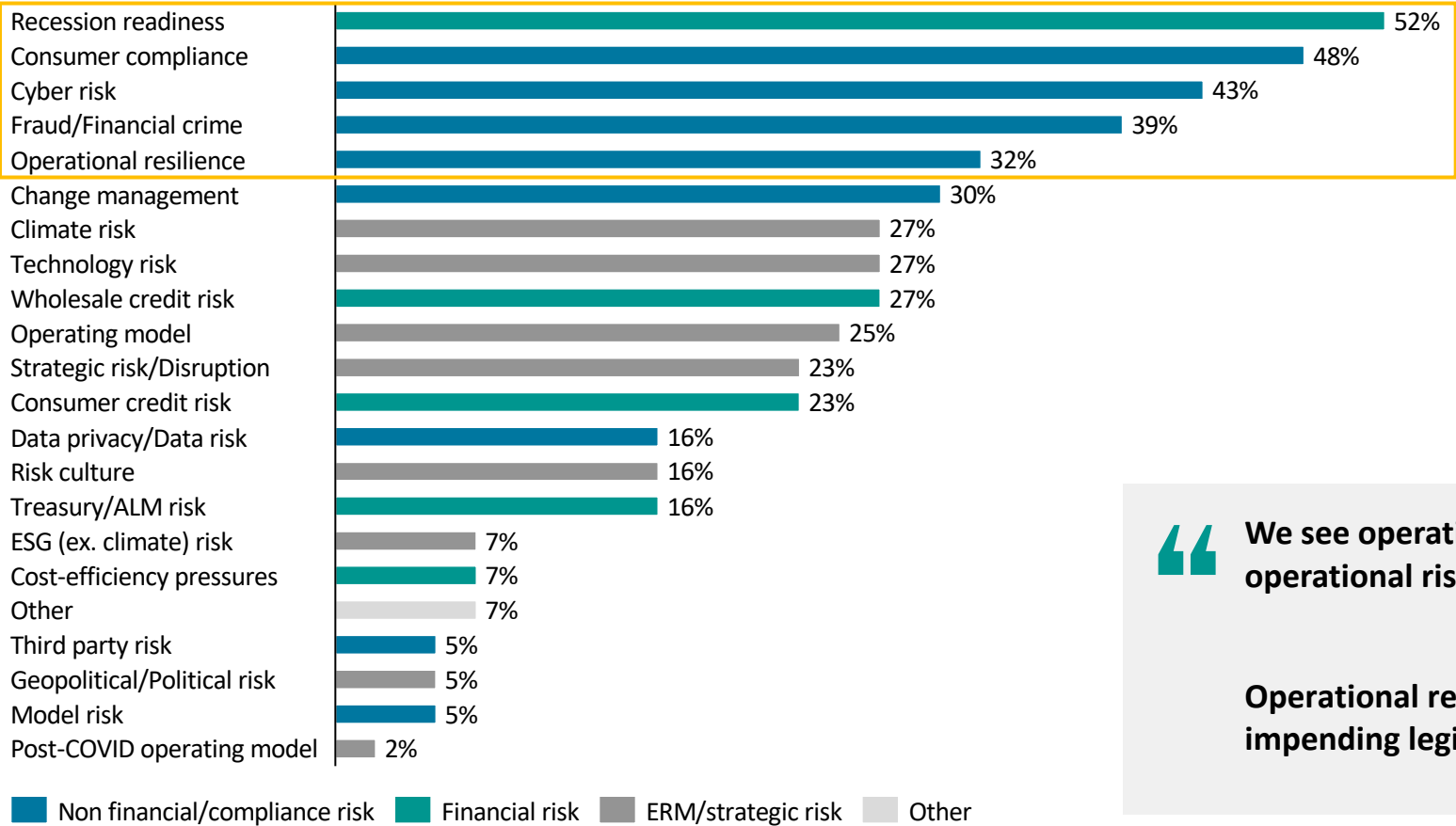
Volatile markets and uncertain macroeconomic environment

Shifting credit cycle	Monitoring and assessing impacts of the shifting macroeconomic environment and geopolitical situation	<ul style="list-style-type: none"> • Closer monitoring and timely response to deterioration of credit quality and provisioning • Use of advanced analytics to spot early signs of credit deterioration • Mitigate model risk posed from IFRS and IRBB models not adequately calibrated to the current macro environment • Increased regulatory scrutiny on leveraged loans, including downgraded corporate loans
Treasury/financial resources	Assessing impacts of the rate environment to liquidity and funding	<ul style="list-style-type: none"> • Review funds transfer pricing (ftp) and asset-liability management frameworks, especially assumptions on client behaviour • Interest rate risk management strategy including structural hedging, IRBB measurement, and scenario forecasting • Review liquidity buffer size and composition in light of redemptions • Ramp up capabilities to support risk-sharing transactions
Operational resilience	Assessing and testing frameworks to mitigate threats to operations and business continuity	<ul style="list-style-type: none"> • Testing and upgrading risk capabilities as part of operational resilience framework, governance, and operating model • Identification of critical business services, assets, and resources, and ensuring resilience across them • Forward-looking views informed by a sound testing framework/capability, third party management
Emerging risks	Timely identification of emerging risks	<ul style="list-style-type: none"> • Increased focus on geopolitical risk • Robust and timely emerging risk identification process with a strong connection into risk appetite • Effective emerging risk processes integrated with existing processes, e.g. stress testing
Business model transition	Ensuring successful transition to a digitised and sustainable business model	<ul style="list-style-type: none"> • Awareness of the threats as well as opportunities of digital transformations, including elevated cyber risks, risks from AI/ML • Digitisation of the risk function itself, including credit workflows, data quality checks, and dashboarding/reporting • Incorporation of ESG-related risks in strategies, objectives, risk appetite, and governance structures • Inclusion of ESG risks across both financial and non-financial risks frameworks
Regulatory agenda	Anticipating developments on the horizon to inform prompt and effective regulatory response	<ul style="list-style-type: none"> • Basel IV – finalise approach and review RWA optimisation while avoiding inflation in cost of compliance • Digital Operational Resilience Act (DORA) – plan for more holistic and strategic approach to ICT risks and threats, including third party risk • Financial crime – new EU regulatory body to counter money-laundering and terrorist financing, the anti money-laundering authority (AMLA) • Trading book controls – increased regulatory scrutiny on trading book controls following Archegos collapse and other events

Source: RMA/Oliver Wyman 2023 CRO Outlook Survey

CHIEF RISK OFFICERS' PRIORITIES

Priorities of risk managers as they look ahead



- Operational risks comprise 4 of top 5 priorities, but only 8 of 21 total
- Operational resilience is Chief Risk Officers' 5th priority
- Non-financial risk accounts for 51% of CRO time overall, but only 40% at the largest banks
 - Time spent on financial risk expected to increase in case of downturn



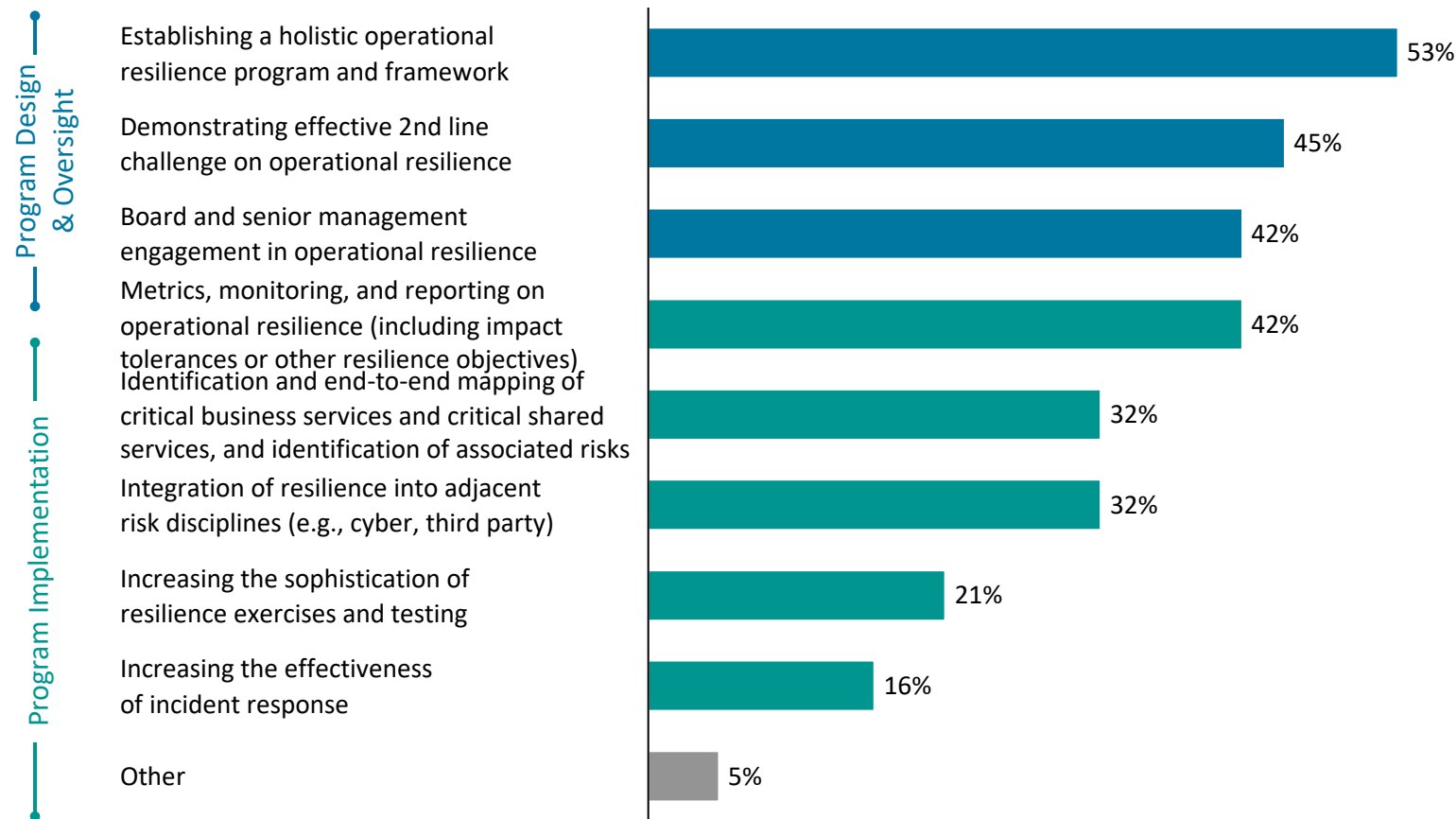
We see operational resilience as the next evolution of operational risk management... it's a more effective approach
– CRO of Major Canada Bank

Operational resilience is a priority, but not because of any impending legislation. We want to stay ahead of the market
– CRO of Vietnam Bank

Source: RMA/Oliver Wyman 2023 CRO Outlook Survey

REGULATOR FOCUS SHIFTING TO IMPLEMENTATION

What CROs see as regulators' focus



1. Australian Prudential Regulation Authority
Source: RMA/Oliver Wyman 2023 CRO Outlook Survey; Celent Interviews with FI Executives

Regulators' focus on operational resilience

- 80% of CROs say regulatory scrutiny for operational resilience has increased in the past year
- 33% say there has been a “significant increase”
- Regulators’ emphasis is shifting from design and oversight toward effective implementation and risk reduction
- Regulators will start looking at effectiveness of resilience exercises, stress testing, and incident response

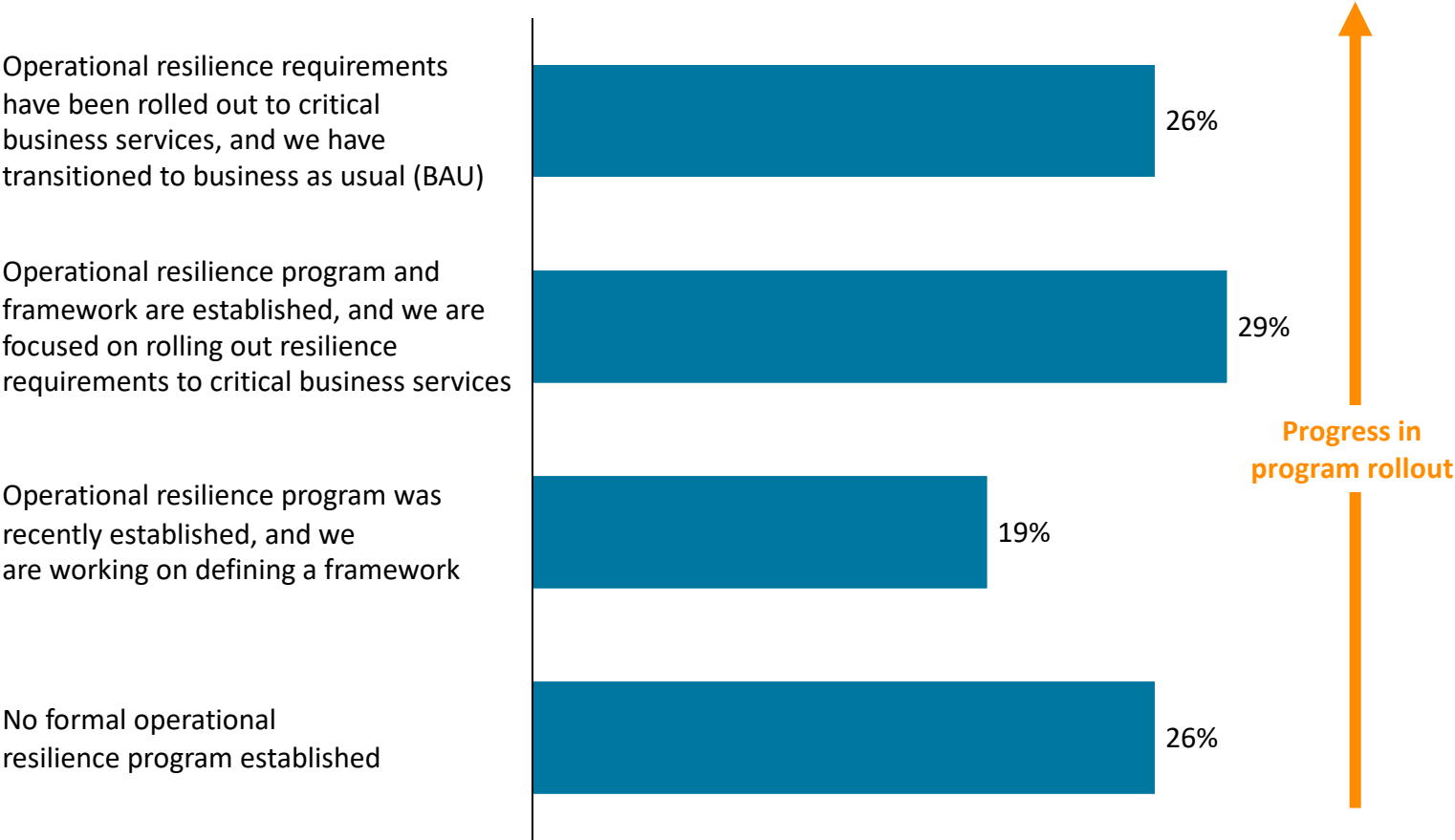


Biggest priority is to do whatever APRA¹ wants

– Former COO, Major Australia Bank

PROGRESS OF OPERATIONAL RESILIENCE PROGRAMS

CROs self-assessment of progress



Transformation to meet operational resilience requirements is underway

- Most banks (74%) are still implementing changes
- 45% are still figuring out how to respond
- Only 26% see themselves as having finished their transformation

Source: RMA/Oliver Wyman 2023 CRO Outlook Survey; Celent Interviews with FI Executives

3

GOVERNANCE, RISK, AND COMPLIANCE SYSTEM TRANSFORMATION

KEY POINTS

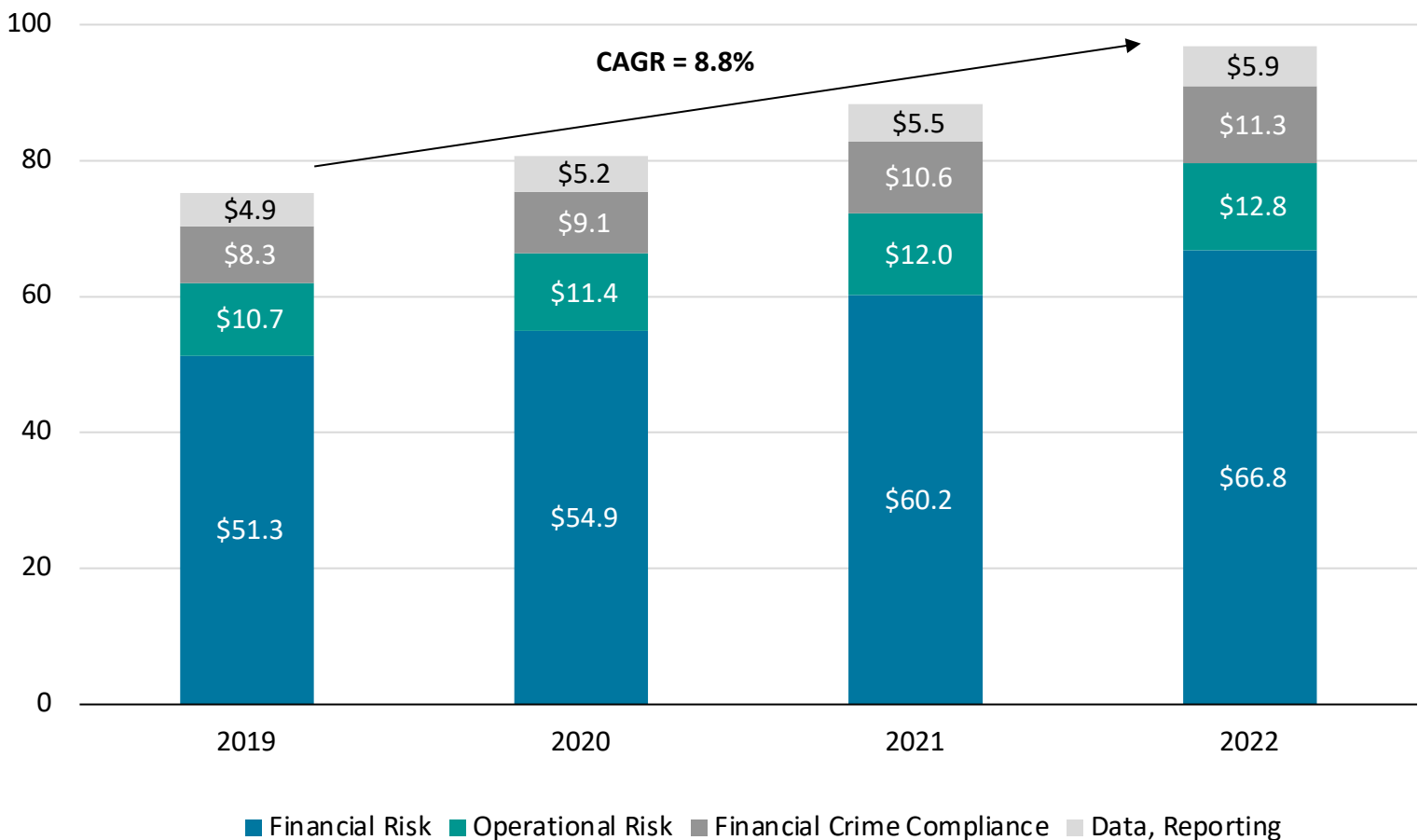
- Operational risk is 14% of risk management technology spend
- Institutions are at different levels of maturity
- All looking for new digital capabilities to accelerate Governance, Risk, and Compliance (GRC) transformation
- We see four different approaches to GRC transformation
- Three approaches enable FIs to operationally manage risk in a coordinated way across the organisation through systems
- The fourth approach requires a robust governance process and people-led processes

OPERATIONAL RISK IS 14% OF RISK MANAGEMENT TECHNOLOGY SPEND

Celent estimates that technology spending by financial institutions on risk management will reach US\$96.8 billion globally in 2023

- Financial risk will account for 69% of the total for functions including market, credit, and liquidity risk; asset-liability management (ALM); and derivatives and hedging
- Operational risk—functions such as GRC and conduct—is 14.2% of the total
- Financial crime compliance will make up 11.7%
- Risk data and reporting will comprise 6.5%

Growth in Global Spending on Risk Technology (US\$ billion)



Source: Celent analysis

INTEGRATING RISK FUNCTIONS TO STRENGTHEN OPERATIONAL RESILIENCE

GRC transformation needed to achieve Integrated Risk Management

GRC’s Role in Integrated Risk Management (IRM)

- GRC systems underpin operational risk programs at financial institutions, providing a platform for tracking and mitigating risks across the enterprise
- OR regulation is leading financial institutions to link up general operational and audit functions, specialised functions like vendor and IT risk, and strategic IRM—and to support them all through one GRC platform
- Operational resilience regulation requires FIs to operationally manage risk in a coordinated way across the organisation

Current State of GRC Use

- Many large financial institutions don’t have integrated GRC systems at group/top level. For most, it is too much to update a single system for all regulatory change requests across business units and across the world
- GRC systems are typically at LoB level, where they can be maintained and updated more flexibly
- Most banks have built global data lakes with reporting tools to combine siloed data, respond to regulator requests and enable holistic analysis of dependencies and risks

Operational Resilience Compliance Requiring IRM



Objectives of GRC transformation

- While many banks have an integrated view of risks, without a consistent GRC system across the bank, they don’t have a systematic way to coordinate response to risks or regulatory requests
- FIs are integrating the operational risk management functions, sometimes on a single GRC platform, to overcome functional silos and change their risk posture on an enterprise-wide basis
- Incumbent GRC platforms support multiple risk functions including ERM, compliance risk, conduct risk, audit, and IT risk. Vendor risk is a newer area of focus. ESG is an emerging area for GRC coverage

Source: Celent analysis

KEY INTERVIEW FINDINGS ACROSS REGIONS



No risk can be looked at in isolation ever. A credit risk has a little bit of op risk, and an op risk has a little bit of market risk

– Deputy Managing Director,
Major India Bank

Getting big GRC systems out is only done by an act of God

– Former COO, Major Australia Bank

Banks are pivoting to a process-led view of risk management because of operational resilience

– Partner, Financial Services Consulting Firm

Operational Resilience

- OR regulation is not driving transformation as strongly in Asia Pacific
- Regulations are less onerous and have taken longer to arrive
- ANZ, Hong Kong, and Singapore are regions where OR is currently driving GRC transformation
- Japan and India have equivalent regulations, but enforcing them is not yet a priority

GRC Priorities

- In addition to compliance, reducing costs through automation and AI is the next priority
- Unlike Europe and North America, we are not seeing either rip-and-replace or build-from-scratch approaches to GRC transformation
- There is a strong desire to keep existing systems in place and build around them (e.g., extract data and use for analytics/reporting)

GRC Technology

- Large institutions don't have integrated GRC systems at group/top level. For most, it is too much to update a single system for all regulatory change requests across business units and across regions
- GRC systems are at LoB level where they can be maintained and updated more flexibly
- Some major institutions still have manual operational risk controls. GRC systems that had the needed breadth of functionality were evaluated and considered too complex
- Most institutions in Japan do not have GRC packages but do have a strong emphasis on managing risk at the first line of defence. The second line of defence often sits in the units

Trends

- ESG risk was recognised by most as a priority, but few firms had a means for managing it
- Almost everyone saw greater accountability for first line as important, but some said it wasn't a priority because they saw first line as already accountable
- Integrated view of risk was surprisingly low on priority list, as some saw it as unactionable – a “dashboard exercise without teeth”
- Third party risk management was on the radar, but not yet a priority

SPECTRUM OF ENTERPRISE-LEVEL APPROACHES TO GRC

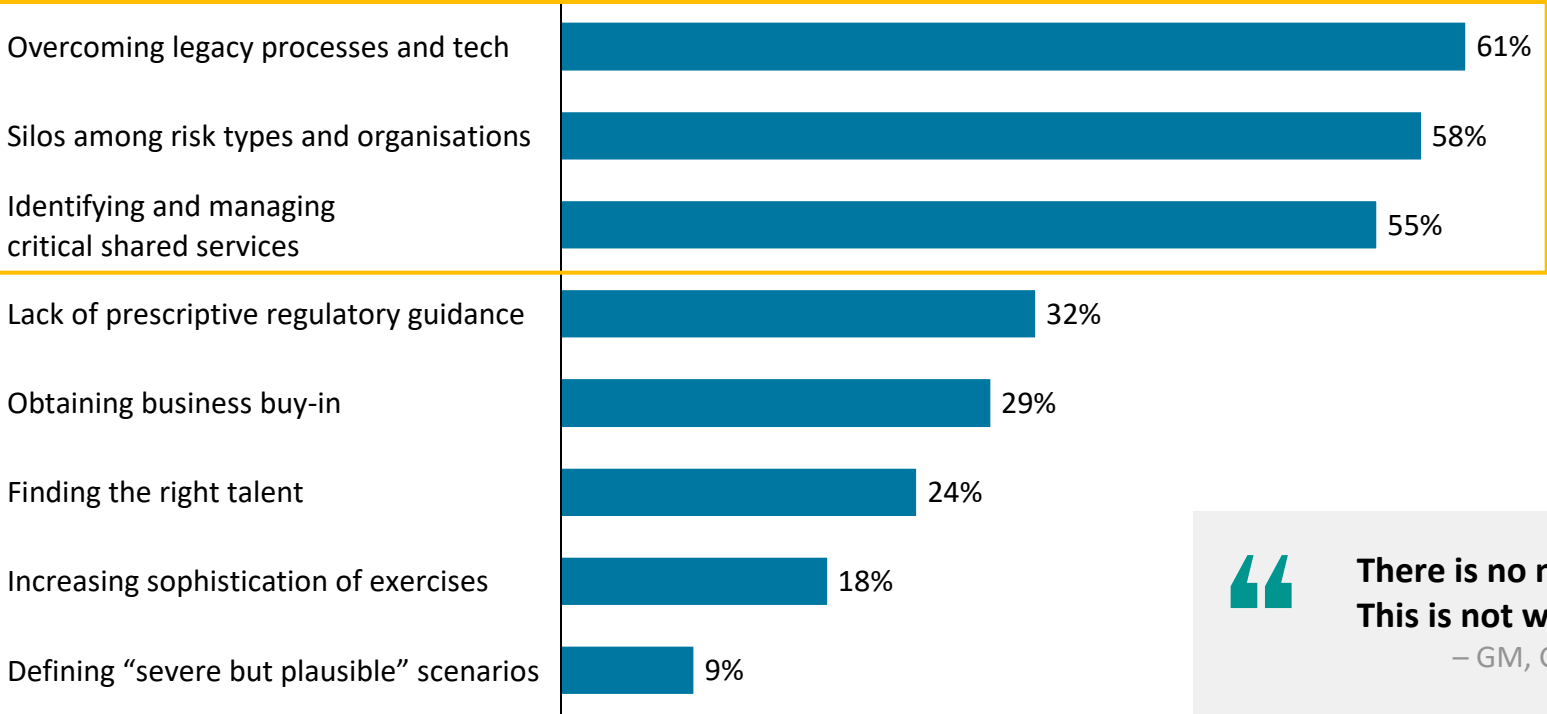
- The financial institutions we interviewed across Asia Pacific were currently using a LoB-led or enterprise-led approach
- Neither of these approaches facilitates managing risk in a coordinated way across the organisation
- This shortcoming is pushing FIs to move to an integrated approach to GRC

Approach	Description	Implications
Reactive	GRC activities are mostly reactive. No centralised approach to manage risks or compliance across lines of business (LoBs). Limited GRC technology. Some reliance on manual processes and spreadsheets.	<ul style="list-style-type: none"> • No visibility into risk above business. Limited analytics • Compliance handled in LoBs
LoB-led	Bank has an enterprise-level approach to GRC, but approaches vary within business units. Varied levels of process and technology maturity across different risk types. No integration across risk types or across risk function within LoBs. It is a large ad hoc effort to build a comprehensive view of risk across the bank. Varied use of basic GRC software solutions in different parts of the bank. Business units and risk types each have their own set of analytics. Potentially there is a uniform, bank-wide approach for a single risk type e.g. cybersecurity.	<ul style="list-style-type: none"> • Enterprise-level views compiled manually • Analytics run on ad hoc basis • Compliance handled centrally, but changes executed in LoBs
Enterprise-led	Bank has a defined GRC framework with a three line-of-defence risk program. CRO uses second line of defence to co-ordinate across the bank. Risk processes are integrated and aligned with the bank's business objectives, but risk management is optimised at business-unit level. Enterprise risk group assesses risk and consolidates reporting across enterprise. There are multiple legacy GRC packages in place, but bank is connecting them to bring output into a single data lake that then can generate consistent reporting and field ad hoc regulatory requests for information.	<ul style="list-style-type: none"> • Data visibility across enterprise • Deep analytics across enterprise • Compliance handled centrally, but changes executed in LoBs
Integrated	Risk management is seen as a performance lever. Bank has achieved a high level of GRC maturity, where risk management and compliance are integrated into business processes, and there is a continuous focus on improving the GRC framework. State-of-the-art GRC program integrated with the bank's business strategy that uses machine learning and automation. Dedicated technology team that supports and develops the GRC program. Advanced risk management solutions use AI and predictive analytics.	<ul style="list-style-type: none"> • Data visibility across enterprise • Deep analytics across enterprise • Regulatory responses can be effected centrally through systems

Source: Celent analysis

ISSUES SLOWING DOWN PROGRESS OF OPERATIONAL RESILIENCE PROGRAMS

Issues hampering progress of Operational Resilience programs



- The top three issues are all impediments to establishing an integrated risk management approach
- Many FI CROs are struggling to integrate the myriad GRC systems that exist across their organisations
- Getting business buy-in from divisions or lines of business also is critical



There is no need to integrate the risks across the enterprise. This is not wanted by management

– GM, Global Business Planning, Japan Life Insurer

Last year, I thought GRC could help integrate, but I could not find an appropriate system

– IT Strategy Director, Japan Insurer

Source: RMA/Oliver Wyman 2023 CRO Outlook Survey; Celent Interviews with FI Executives

OPERATIONAL RESILIENCE AND RESPONSE: AUSTRALIA



AUSTRALIA

CPS 230: Operational Risk Management

Regulators: APRA¹

Timing: Finalisation expected mid 2023
Becomes effective 1 January 2025

Objective: Strengthen the management of operational risks in the banking, insurance, and superannuation industries



Main problem with buying a single integrated GRC system for a large-scale bank ... Regulator comes with new regs, vendor tells you it isn't on road map, so you have build a bespoke tool to deliver on regulator's timeline

– Former Global CRO, Major Australia Bank

Biggest priority is to do whatever APRA wants

– Former COO, Major Australian Bank

Notes on Operational Resilience and GRC:

- Big four banks are among the most mature in terms of operational risk management, but primary responsibility is in line of business
 - Still knitting integrated views together at group level
 - Extracting risk data from LoBs, housing in global data lake, and putting reporting tools on top
- In the middle of substantial GRC transformation
 - Still responding to operational risk changes kicked off as a result of Royal Commission. Investing in GRC is concrete evidence that they are taking required action
 - Waiting on finalisation of CPS 230 to understand what further changes need to be made for operational resilience
- Big banks trying to move all systems supporting business units (including GRC) onto the cloud
- Smaller banks are either moving to end-to-end GRC systems or using what is included in their core banking system
 - CPS 230 is due to be effective by 1 Jan 2025. APRA will look to Big four to comply first
 - Operational resilience may be opportunity for stand-alone GRC system if incumbent systems not updated quickly and APRA begins to push for compliance

1. Australian Prudential Regulatory Authority
Source: Primary Interviews, Celent analysis

OPERATIONAL RESILIENCE AND RESPONSE: INDIA



INDIA

Master Direction on IT Outsourcing

Regulators: Reserve Bank of India

Timing: Issued June 2022

Objective: Ensure that Regulated Entities (REs) outsourcing arrangements don't impact customer service and that they are subject to regulatory supervision

Market Structure:

Banks fall into one of three categories for GRC maturity

1. *Compliant Players* – Only do what is necessary. Just interested in getting franchise out of danger from regulatory penalties. This is 2/3 of Indian banks
2. *Leaders* – Incremental improvements over what's required. Using better risk analytics. Have embedded risk into governance and have unified enterprise-wide risk management and operational risk management systems. This is 1/3 of banks
3. *Visionaries* – Gather international and local best practices. Get ahead of emerging risks. Use advanced data and predictive analytics. Info security goes beyond mandated protocols. This is only the three banks identified as SIFIs – SBI, ICICI, HDFC



GRC in India has different maturity levels than the West

– Deputing Managing Director, Major India Bank

Notes on Operational Resilience and GRC:

- Indian banks are very mature in terms of financial risk management, but operational risk management is still a new capability
 - Indian banks are through the most dramatic change in ages as more and more money flows into banking system
 - Risk management is digitising as they introduce analytics, early warning systems
- First line and third line of defence are mature – risk managed competently in the business units and the audit practices are well formed
- Second line of defence is relatively new in Indian banks
 - Banks using second line as value creation capability rather than solely for governance.
 - Second line is sometimes used as a centre of excellence to improve first line operational risk management
 - Getting second line up to full functionality is critical to relieve pressure on first and third lines
- High focus on using algorithms and data in operational risk management
- Biggest banks want to have best-in-class technology for major modules; as a result, they need a distinct system for integrated risk management
- Lots of opportunity in GRC transformation with international banks' local subsidiaries as they seek local regulatory expertise

OPERATIONAL RESILIENCE AND RESPONSE: JAPAN



JAPAN

Ensuring Operational Resilience Discussion Paper

Regulators: Japan Financial Services Authority (JFSA)

Timing: Paper released 16 December 2022

Objective: Present a framework for ensuring operational resilience based on an overview of international trends, and set out issues to be considered



There is no need to integrate the risks across the enterprise. This is not wanted by management

– GM, Global Business Planning, Japan Life Insurer

GRC-style operational risk functions are not done on a system basis in Japanese banks

– Senior Director, Banking Systems

Risk management, governance/control, compliance management are all separate. The firm does not see this as a problem

– IT Strategy Director, Japan Insurer

Notes on Operational Resilience and GRC:

- Japan most buttoned up in terms of seeing operational resilience processes as being complete
 - FIs see themselves as already very operationally resilient due to earthquakes and monsoons
 - Regulators are as focused on operational resilience as they were pre pandemic
- Japanese regulatory regime is more cooperative than confrontational
 - Regulators are not as active in enforcement in Japan
 - Therefore, they will not be as central to driving GRC transformation
- GRC systems are not seen as a panacea
 - Most FIs in Japan do not have GRC packages but have a strong emphasis on managing risk at the first line of defence. Second line of defence sits in the units
 - In the insurers we interviewed, risk policy and controls were on spreadsheets
 - Consultants to Japanese banks confirmed that most domestic banks are on manual systems, even while their foreign subsidiaries have implemented GRC software
 - Proliferation of data privacy rules is prompting them to look at GRC systems
- Biggest GRC priority is agent conduct and fraud, where every new sale must be verified by second line of defence in order to sell new business
- Cybersecurity is one area where firms are looking for integrated approach
- FIs are investing in ESG capabilities and even creating new departments

OPERATIONAL RESILIENCE AND RESPONSE: SOUTHEAST ASIA



SOUTHEAST ASIA

Business Continuity Management Guidelines

Regulators: Monetary Authority of Singapore

Timing: Revised June 2022

Objective: Introduce principles and practices that financial institutions can implement to strengthen their operational resilience



Technology allows Tier 2s to catch up to the G-SIBs and perform the same with much smaller budgets

– CRO, Major ASEAN Bank

Operational resilience is a priority, but not because of any impending legislation. We want to stay ahead of the market

– CRO, Vietnam Bank

People think of operational risk as a boring librarian with big teeth, but it is at heart of digitisation






– CRO, Vietnam Bank

Notes on Operational Resilience and GRC:

- Singapore is only government to issue regulations specific to operational resilience
- Singapore also seen as second most mature in terms of GRC capabilities after ANZ
- Regulators in other SEA countries primarily focused on capital controls and financial risk
- Maturity outside of Singapore is low due to lack of regulator focus on operational risk
- Banks operating in SEA more inclined to a centralised risk management approach due to the number of countries they operate in
 - They rely on single centres of excellence in Singapore for risk and technology, then service other countries from there
- CROs view operational risk management primarily from lens of how does it improve the business
 - Primary focus on embedding it into the first line of defence
 - Looking to automate second line of defence as much as possible to reduce error and make sure operational risk isn't inefficient
 - One bank using issue tracking software (Jira) as primary GRC software

EMERGING CLIENT REQUIREMENTS FOR GRC PLATFORMS

Digital technologies will provide much-needed enhancements to GRC capabilities

Digital Technology	Client Requirements	GRC Use Case
 Artificial Intelligence	<ul style="list-style-type: none">• Predictive analytics, natural language processing, natural language generation• Soon clients will be looking for use of LLMs	<ul style="list-style-type: none">• AI and machine learning to support advanced analytics of risk trends, including early warning• NLP and LLMs to support the auto-interpretation, classification, and scoring of qualitative risk assessments entered by end users• NLG to auto-create mitigation plans, including plans for new risks and events
 Robotic Process Automation	<ul style="list-style-type: none">• Automation capabilities to replace sneakernet currently used to span different systems within the risk management and GRC capabilities	<ul style="list-style-type: none">• Extraction of control execution from process workflows• Knitting together risk reporting data from LoBs to generate dashboards for board and C-suite
 Usability	<ul style="list-style-type: none">• Software and interfaces non-risk employees are familiar with to increase first line participation in risk management	<ul style="list-style-type: none">• Using employee familiarity with issue tracking and ticket management software in IT risk management to increase employee risk incident reporting
 Low-Code/No Code	<ul style="list-style-type: none">• Second line of defence can easily alter systems to reflect changes in process or changes in workflows required for compliance and risk management	<ul style="list-style-type: none">• Develop risk assessment forms, surveys, and questionnaires to collect data from business users and automate risk scoring• Create workflows to track compliance requirements and generate reports• Update vendor onboarding, risk scoring, and due diligence processes
 Data Fabric, Data Wrangling	<ul style="list-style-type: none">• Ease of extracting data from GRC systems• Ease of integrating with modules from other vendors (particularly those outside core GRC)	<ul style="list-style-type: none">• AI-based linkage of data from disparate systems to provide holistic, enterprise-wide analysis of dependencies and risks• Easy integration with Diligent to automate upload of risk reports to board

Source: Celent analysis

FOUR APPROACHES TO GRC TRANSFORMATION

The first three approaches all enable FIs to manage risk and compliance in a coordinated way through systems. The Extract and Compose approach requires coordinating through governance meetings and people-led processes

Approach	Description	Advantages	Disadvantages
1. Build your Own	Build own GRC program based on need for unique capabilities and conviction that packaged systems will not suffice. Requires deep data architecture skills and extensive development arm.	<ul style="list-style-type: none"> Bespoke software meets business's specifications and unique requirements 	<ul style="list-style-type: none"> Order of magnitude more difficult and expensive than other approaches Timing and ultimate success is uncertain
2. Rip and Replace	Choose single package that all units and geos are required to migrate to. Staged implementation by geo or unit. Requires very strong and persistent enterprise-level governance to approve and implement project.	<ul style="list-style-type: none"> Consistent, uniform capability across organisation Once implemented provides integrated view of risk that allows second line to zoom in or out across organisation Single control library and single database eliminates redundancy 	<ul style="list-style-type: none"> High execution risk as moving every unit onto a new system requires customisation to build required functionality for units Maintenance costs
3. Focus on Core	Put core capabilities on single package (<i>regulatory change, policy and compliance, operational risk</i>). Use best-of-breed for non-core (<i>audit, legal, third party risk, ESG, BCP</i>). Requires strong and persistent enterprise level governance.	<ul style="list-style-type: none"> Provides integrated view of risk, single control library, unified database of risk data Easier to manage stakeholders Allows LoBs to have keep some of their systems More focused implementation 	<ul style="list-style-type: none"> While lower than Rip and Replace, execution risk is still considerable
4. Extract and Compose	Keep legacy packages in place in LoBs. Extract data into global data lake. Run analytics on extracted data. Place reporting tool on top to respond to regulatory requests, generate reports. Requires data transformation skills.	<ul style="list-style-type: none"> Very flexible for responding to regulators Consolidate analytics Stakeholders get to keep systems that work for them 	<ul style="list-style-type: none"> Still need to maintain multiple systems Difficult to change underlying processes based on insights

STARTING STEPS FOR AN EFFECTIVE OPERATIONAL RESILIENCE PROGRAM

1.

ESTABLISH THE FOUNDATION

- Establish the program to drive resilience improvements based on lessons learned from the pilot and identified areas of enhancement
- Expand the program to enhance capabilities and roll out a resilience approach across the remaining critical service

2.

PROVIDE VISIBILITY FOR THE BOARD

- Run a pilot on one critical service to enhance resilience:
 - Identify key dependencies and assess risks
 - Define impact tolerances and evaluate resilience through scenarios
 - Craft an improvement road map
- Identify key learnings and program enhancements to facilitate the rollout of the program more broadly

3.

FOCUS ON A SINGLE CRITICAL SERVICE

- Define the target resilience maturity ambition for the organisation
- Identify an initial set of metrics (including resilience program metrics) to provide ongoing reporting to the board

4.

EXPAND THE PROGRAM

- Assign accountability and develop an operating model for resilience
- Conduct a resilience maturity assessment to establish a baseline of the organisation's capabilities
- Articulate the organisation's critical business services

APPENDIX

OPERATIONAL RESILIENCE REGULATION IN ASIA PACIFIC (1/3)



AUSTRALIA

CPS 230: Operational Risk Management

Regulators: APRA¹
Timing: Finalisation expected mid 2023
Becomes effective 1 January 2025
Objective: Strengthen the management of operational risks in the banking, insurance, and superannuation industries

Key Operating Requirements

- Operational risk management has three clear lines of accountability: the board, senior management, and business lines
- Business Continuity Planning (BCP) must be current and appropriate to the nature, complexity, and size of the entity
- Identify material service providers which the bank relies on to perform critical operations

Notes

- Material service providers includes third and fourth party providers
- Includes identification of critical operations and scenario testing like DORA and UK regulations



HONG KONG

Supervisory Policy Manual (SPM) module OR-2 on Operational Resilience

Regulators: Hong Kong Monetary Authority
Timing: Issued May 2022
Develop Operational Resilience Framework by 31 May 2023
Implement framework no later than 31 May 2026
Objective: Provide guidance on the principles that Authorised Institutions (AIs) should consider when building their operational resilience.

Key Operating Requirements

- Banks must view operational resilience as a strategic growth imperative
- Board and Senior Management need to confirm to HKMA that the bank is “operationally resilient”
- Includes requirements to identify critical business services, set tolerances for disruption, map end-to-end dependencies, and implement incident management
- Third party management included under mapping and managing dependencies

Notes

- Very similar to other countries’ regulations except for near-term deadline for establishing a resiliency framework

1. Australian Prudential Regulatory Authority
Source: Regulatory authority publications, legal analyses, Celent analysis

OPERATIONAL RESILIENCE LEGISLATION IN ASIA PACIFIC (2/3)



SINGAPORE

Information Paper on Management of Third Party Arrangements

Regulators: Monetary Authority of Singapore
Timing: Issued August 2022, effective immediately
Objective: Ensure that Regulated Entities (REs) outsourcing arrangements don't impact customer service and that they are subject to regulatory supervision

Key Operating Requirements

- The MAS guidance requires a comprehensive due diligence process for third party providers
- Contractual arrangements with third party service providers should include provisions for risk management, security, and confidentiality
- Action required of FIs is to benchmark their practices against the information paper and take steps to address any gaps in a risk-appropriate manner

Notes

- MAS encourages non-bank financial institutions to adopt the good practices in the paper



SINGAPORE

Business Continuity Management Guidelines

Regulators: Monetary Authority of Singapore
Timing: Revised June 2022, 1 year to implement
Objective: Introduce principles and practices that financial institutions can implement to strengthen their operational resilience

Key Operating Requirements

- Identify critical business services and determine recovery strategies and resource allocation
- Establish a Service Recovery Time Objective (SRT0) for each critical business service
- Identify and map end-to-end dependencies, including third parties
- Audit Business Continuity Management (BCM) framework once every three years
- Require senior management to provide an annual attestation to the board on the state of the FI's BCM preparedness

Notes

- Shift the focus of BCM from individual business functions to a service-centric approach that crosses functions

OPERATIONAL RESILIENCE LEGISLATION IN ASIA PACIFIC (3/3)



INDIA

Master Direction on IT Outsourcing

Regulators: Reserve Bank of India
Timing: Issued June 2022; Goes into effect October 2023
Objective: Ensure that Regulated Entities (REs) outsourcing arrangements don't impact customer service and that they are subject to regulatory supervision

Key Operating Requirements

- Establish board-approved IT outsourcing policy
- Ensure that the service provider's standard of care is on par with RE's own
- Set up a robust grievance redressal mechanism so responsibility for redressal of customers' grievances rests with REs
- Require that service providers have a robust BCP and DRP
- Require that service providers report any incidents, including cybersecurity incidents, within one hour of detection

Notes

- Not as broad as other OR regulations as only pertains to third party risk management and more specifically to outsourcing services



JAPAN

Ensuring Operational Resilience Discussion Paper

Regulators: Japan Financial Services Authority (JFSA)
Timing: Paper released 16 December 2022
Objective: Present a framework for ensuring operational resilience based on an overview of international trends, and set out issues to be considered

Key Operating Requirements

- Identify critical operations
- Set tolerance for disruption for each of them
- Map the interconnection of critical operations, and secure necessary resources
- Verify and test appropriateness to ensure that expected impacts of disruptions are within the tolerance levels set

Notes

- Although primarily directed at banks, also intended to be used by critical third parties
- JFSA will use the Discussion Paper to promote dialogue with FIs, but it does not formally apply individual requirements or use them as checklists in the inspection and supervision of financial institutions

ABOUT CELENT

For over 20 years, Celent has helped senior executives make confident decisions around their technology strategies to execute at scale.

As the financial services industry rapidly evolves, there is more complexity, with new regulations, startups, technologies, and applications to stay on top of and prioritise. Celent helps you connect this ever-changing puzzle. We offer objective advice and clarity, backed by a database of thousands of solutions and award-winning global best practice use cases. With real-life domain expertise, we also guide you through the maze of emerging tech in the pursuit of value.

Our people, data, insights, and relationships form the foundation for you to use Celent to make confident technology decisions in financial services.

We are part of the Oliver Wyman Group, a wholly-owned operating unit of Marsh McLennan [NYSE: MMC].

ABOUT SERVICENOW

ServiceNow (NYSE: NOW) makes the world work better for everyone. Our cloud-based platform and solutions help digitise and unify organisations so that they can find smarter, faster, better ways to make work flow. So employees and customers can be more connected, more innovative, and more agile. And we can all create the future we imagine. The world works with ServiceNow®. For more information, visit www.servicenow.com.

© 2023 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.