WHITE PAPER

Operational Resilience 2025

NAVIGATING THE GLOBAL REGULATORY LANDSCAPE IN 2025 AND BEYOND

riskonnect.

January 2025

Executive Summary

Organizations today know the importance of planning for the unexpected. The rise of cyberattacks, supply-chain disruptions, extreme weather disasters, and geopolitical instability are a few examples of the disruptions organizations and governments have to contend with.

So much disruption has led to a broader consensus on what it means to be operationally resilient. The financial services sector continues to lead the charge in defining what operational resilience is and how to achieve it. While few industries are mandated to comply with operational resilience requirements, all organizations should consider applying these principles to become more resilient.

This white paper, updated for 2025, will help your organization become more operationally resilient to thrive during uncertain times. You'll learn how to:

- Navigate different perspectives specified by regulation around the globe.
- Identify common best practices.
- Apply these concepts in a practical way.

Operational Resilience at a Glance

While many of the practices highlighted in this white paper originated with regulations in the financial sector, they are universally applicable to any organization wishing to develop operational resilience:

1. Identify your most important business services and critical operations.
2. Set impact tolerances.
3. Conduct service mapping and identify dependencies and interconnections.
4. Identify and test against plausible scenarios.
5. Integrate third-party risk management into resilience initiatives.
6. Improve information and communication technology and cyber resilience.

Table of Contents

Executive Summary: Operational Resilience – Navigating the Global Regulatory Landscape 2

Introduction 4

Resilience Themes 5

- Identify Business Services and Critical Operations 6
- Set Impact Tolerance 8
- Conduct End-to-End Mapping and Identify Interconnections 10
- Identify and Perform Testing of Plausible Scenarios 12
- Integrate Third-Party Risk Management into Resilience Initiatives 14
- Improve Information and Communication Technology and Cyber Resilience 16

Case Study 18

Requirements, Regulations, and Best Practices 24

- Australia (APRA) – Operational Risk Management 25
- European Union – Digital Operational Resilience Act 26
- Global (Basel) – Principles for Operational Resilience 27
- Hong Kong SRA (HKMA) - Operational Resilience 28
- Ireland (CBI) – Operational Resilience 29
- Singapore (MAS) – Guidelines on Business Continuity Management 30
- United Kingdom (PRA/FCA) – Operational Resilience 31
- United States (OCC, Federal Reserve, FDIC) – Sound Practices to Strengthen Operational Resilience 32
- Canada (OSFI) – Operational Resilience and Operational Risk Management 33

Conclusion 34

Introduction

Operational resilience is the ability of an organization to deliver its services through disruption. It includes proactively identifying and mitigating single points of failure and vulnerabilities, as well as developing capabilities to effectively respond to disruption and remain within approved impact tolerances.

In the past few years, there has been a significant push by regulatory bodies to define operational resilience and develop best practices to avert pain and disruption to the customer and the market.

For some, regulation can be seen as an opportunity to put in place safeguards that protect the customer, the business, and the wider market. Others, however, see regulation as a hindrance to the rapid delivery of products and services to customers and markets. While the need for regulation can be debated, one outcome is clear – regulatory pushes in the financial sector have forced organizations to examine how they deliver their most important business services, build resilience in their operations, and in many cases, how continuity planning is being conducted.

This white paper examines practices introduced through various regulations in the financial sector, reviews the commonalities and differences between regulations, and highlights best practices that can be applied to all sectors, regulated or not.

In the end, effective operational resilience helps ensure that disruption does not lead to widespread impacts on markets and customers – or result in firms being unable to continue their operations.

Resilience Themes

Resilience Themes

Achieving operational resilience is challenging, particularly for those organizations that operate across geographic and regulatory jurisdictions with multiple supervisory requirements to administer. While there are numerous requirements that are often intertwined, there are common themes and best practices that can help regulated – and unregulated – organizations build a more resilient enterprise and evolve existing (traditional) continuity programs.

Identify Business Services and Critical Operations

Before you can start prioritizing actions to improve operational resilience, you must define the most important services your organization delivers to its customers. This will focus resilience efforts and provide a "north star" to scope resilience activities.

Regulations use a variety of terms to refer to this concept, including important business services, critical operations or functions, and products and services. Whatever the exact terminology, the meaning is clear: Organizations must define those strategic, top-level services that are significant enough that their disruption could cause excessive harm to customers and markets – or even lead to an organization's failure.

> **Important business services are outcomes delivered by an organization, which, if disrupted, could cause catastrophic impacts for the market, organization, and customers.**

Regulatory Similarities and Differences

Regulations refer to important services in different ways. For example, APRA (Australia), HKMA (Hong Kong) and OCC/FDIC (US) use the term "Critical Operations," defined as those operations and their associated services whose failure or discontinuance of which would pose a threat to financial stability.

FCA/PRA (UK) and CBI (Ireland) use "Important or Critical Business Services" (IBS), which are those services that, if disrupted, could cause intolerable harm to a firm's customers or pose a risk to the stability and resilience of the financial system (or financial markets).

While the terms may vary, all refer to a similar concept – important business services or critical operations deliver value-added outcomes that, if disrupted, create intolerable harm for customers, organizations, and markets.

UK regulators outline 13 factors[1] that firms should consider when selecting their important business services.

1. The nature of the client base, including any vulnerabilities that would make the person more susceptible to harm from a disruption
2. The ability of clients to obtain the service from other providers (substitutability, availability, and accessibility)
3. The time criticality for clients receiving the service
4. The number of clients to whom the service is provided
5. The sensitivity of data held
6. Potential to inhibit the functioning of the UK financial system
7. The firm's potential to impact the soundness, stability, or resilience of the UK financial system
8. The possible impact on the firm's financial position and potential to threaten the firm's viability where this could harm the firm's clients or pose a risk to the soundness, stability, or resilience of the UK financial system or the orderly operation of the financial markets
9. The potential to cause reputational damage to the firm, where this could harm the firm's clients or pose a risk to the soundness, stability, or resilience of the UK financial system or the orderly operation of the financial markets
10. Whether disruption to the services could amount to a breach of a legal or regulatory obligation

[1] Factors are outlined in the FCA's SYSC 15A.2.4. Lloyd's Market Association (LMA), an association to help the underwriting community, also provides insights on these 13 factors to consider when identifying IBS.

11. The level of inherent conduct and market risk
12. The potential to cause knock-on effects for other market participants, particularly those that provide financial market infrastructure or critical national infrastructure
13. The importance of that service to the UK financial system, which may include market share, client concentration, and sensitive clients

While these highlight potential damage to financial markets, the concepts can be applied to other industries to help organizations select important business services.

In Perspective

A few shared characteristics are relevant to both regulated and nonregulated companies when defining IBS (or critical operations):

- Less is more. The fewer services that are deemed important, the more you can focus on the resilience of those services considered in-scope. The number of services deemed important is commensurate with the size and complexity of the organization.
- IBS need to be defined so they have a distinct, repeatable outcome and an associated impact tolerance or downtime.
- IBS should be distinct enough to allow the identification of plausible scenarios that could affect delivery. Defining plausible scenarios will help with scenario testing.
- Generally, the bucketing of services under one IBS should be avoided, but this may be necessary for nonregulated organizations, such as manufacturing. In this case, one will need to look for services that produce similar outcomes, have similar resources required for delivery, and share common impact tolerances.
- Start with external-facing services that are likely to affect markets and customers. Then consider those services that are required for continued operations or to maintain safety or soundness for the organizations.
- Be aware that regulations differ by jurisdiction on whether internal services should be considered.

> Identifying important business services spotlights those outcomes that must be protected so organizations can focus their resilience and continuity efforts and create transparency around what's truly important.

[2] There is a lot of debate between whether organizations should include internal services at all. Some regulations, such as operational resilience requirements in the UK and Ireland, are specific in stating that only external-facing services should be considered. Other jurisdictions are vague and leave it up to the discretion of the organization.

Set Impact Tolerance

In a joint publication, the PRA and FCA defined an impact tolerance as "the maximum acceptable tolerable level of disruption to an important business service or an important group of business services as measured by a length of time in addition to any other relevant metrics."

At their core, impact tolerances represent lines in the sand that organizations do not want to cross because the consequences could be intolerable for customers, markets, or the organization itself. The most common metric used for impact tolerance is a timeframe, but other metrics, like the number of unresolved customer complaints, can (and should) be used.

> Impact tolerances are the point in time – or decreased capacity of – when disruptions to an important business service causes unacceptable harm to a customer, the broader market, or irrevocably threatens an organization's viability.

Regulatory Similarities and Differences

The term "tolerance" is used in some regulations while "impact tolerance" is used in others. For example, Basel, DORA, and the U.S. all use a more general definition of tolerance based on operational risk practices. Tolerance is "the level of risk an organization is willing to accept given a range of severe but plausible scenarios." Regulation in the UK, Ireland, and Australia is direct in requiring that impact tolerances have a time component and potentially other metrics, such as data loss. Regulators in Canada (OSFI) also recently introduced the concept of a "tolerance for distruption" to further complicate the issues which includes a time component with considerations for other factors, such as "diminishment of service, loss of data, or extent of customer impact."

While all approaches have value, the idea of impact tolerance, inclusive of discreet timeframes and other metrics, provides the most value for resilience and continuity practitioners since it is empirical and measurable. MAS (Singapore) is unique in that it introduces the idea of a service recovery time objective, but this is defined as a time-based metric associated with a service, similar to the concept of an impact tolerance.

In Perspective

Here are a few best practices that are applicable to both regulated and nonregulated organizations establishing impact tolerances:

- Impact tolerances must have a time component to them and should have other metrics where it makes sense.
- Impact tolerances are different from recovery time objectives (RTOs). RTOs represent an objective and are usually assigned at the activity, process, or resource level. Impact tolerances aren't just objectives; they represent thresholds that shouldn't be exceeded and are set at the service level.
- Impact tolerances require both quantitative data and qualitative input to determine. There is no magic bullet in terms of the perfect formula that will set impact tolerances for you. It is art more than science.
- When developing qualitative criteria, it is helpful to leverage existing risk frameworks and rubrics. When done well, this can also help bridge the gap between concepts of impact tolerance and risk tolerance.
- Setting impact tolerances requires senior leadership input. For regulated organizations, this is non-negotiable. For nonregulated entities, senior leadership buy-in, although not mandatory, remains critical.
- Once set, impact tolerances become the baseline for future capability reporting. Setting impact tolerances can help move your organization from compliance-based metrics to capability-based metrics.

> Assigning impact tolerances creates consensus on what resilience capabilities an organization needs to have in place to avoid intolerable harm to customers, markets, and the organization. By determining impact tolerances for each IBS, organizations can draw a line in terms of risk and disruptions they are willing to tolerate.

Conduct Service Mapping and Identify Dependencies and Interconnections

Once an organization understands its most important business services and identifies appropriate impact tolerances, it can map its IBSs from beginning to end. Regulatory requirements are similar in stating what resources need to be considered. These include identifying the people, technologies, processes, data, facilities, third parties, interconnections, and dependencies between all resource types. The goal of mapping your services is to gain a better understanding and clearer visibility of all the resources required for service delivery and, ultimately, to be able to identify where there may be single points of failure, limited redundancies, or concentration risk.

> Service mapping is the process by which an organization identifies the people, technologies, information, facilities, third parties, and processes required to deliver an important business service and uses that information to determine where risks and single points of failure exist.

Regulatory Similarities and Differences

While the core categories (data, people, premises, suppliers, and technology) of resources to be catalogued during mapping activities are largely similar between different regulations, organizations differ in their use of existing materials to assist in service mapping activities. For example, those regulated by FCA/PRA (UK) have been more likely to consider service mapping as its own activity, distinct from processes like conducting a business impact analysis or operational risk analysis.

Other firms have opted to expand on existing program materials. OCC guidance and guidance from MAS build on existing business continuity processes. For example, the OCC notes that the "firm leverages both mapped interconnections and interdependencies of its critical operations...set forth in its recovery or resolution plans, as well as relevant business impact analyses." Basel and the APRA see dependency mapping as an extension of operational risk practices. There is no right answer, but using existing data can provide a tremendous head start.

In Perspective

Service mapping clarifies what is required to deliver important business services. There are a few best practices:

- Mapping should catalog resources across five pillars, including people, processes, technology, facilities, and information. Interdependencies between the pillars also need to be identified.
- Organizations should use existing materials from business continuity programs where possible, but the information may need to be modified to be used for end-to-end mapping.
    - BIAs are often written from the perspective of what the business needs and may lack details around resources required for service delivery. This can particularly be the case for any technology or IT-focused BIAs.
    - Information collected from a BIA may need to be one level deeper. For example, an organization may use a third party for multiple services, and these details may need to be captured to show which services delivered by the third party are required for which IBS.
- More isn't necessarily better. Many organizations produce spreadsheets and mapping documents so detailed and complex they are unable to see trends and patterns or identify
- Having a system to manage all the interconnections is essential. This will help develop a digital map of the organization.

> Service mapping allows an organization to see all the processes and resources necessary to deliver an IBS or critical operation to a customer or stakeholder. When done well, mapping allows organizations to see where processes are likely to fail or where there are single points of failure or vulnerabilities. These weak spots can be targeted for risk mitigation or used in the development of plausible scenarios.

Identify and Perform Testing of Plausible Scenarios

Developing severe, yet plausible scenarios is a core element of operational resilience thinking. Scenarios are used to develop testing plans and provide concrete examples of situations that could cause an organization to exceed its impact tolerances. When plausible scenarios are designed based on risks identified during mapping exercises, these scenarios help:

- Prioritize risk remediation.
- Improve the quality of contingency planning.
- Inform the development of testing plans.

Using plausible scenarios to develop testing plans helps organizations understand the most appropriate type and frequency of scenario testing and allows for more robust and tailored planning. The testing plan will need to include details on how it will gain assurance that the organization can remain within the impact tolerances for each of its important business services.

> Plausible scenarios are realistic events that could disrupt the delivery of a business service's outcomes leading to unacceptable impact. Plausible scenarios should be severe; they should prevent an organization from being able to recover within service-specific impact tolerances.

Regulatory Similarities and Differences

Scenario testing can have multiple meanings, depending on the context and source. In the operational resilience space, scenario testing is used to validate that an organization can remain within its impact tolerances when faced with extreme, yet plausible scenarios and the risks and threats they introduce. This is in contrast to traditional stress-testing practices, which focus on how firms respond to market conditions and financial stress.

The FCA/PRA document outlines specific guidance of the types of scenarios that should be covered, including disruption to the data required to deliver an IBS, unavailability of facilities or key people, unavailability of critical third parties, disruption to market participants, and loss of technologies to deliver IBS. APRA provides additional guidance that scenarios should include disruptions that require contingency arrangements. All regulations note the value of using scenarios as part of a testing plan and validating that organizations can remain within impact tolerances.

In Perspective

Developing and testing plausible scenarios are activities that will grow and mature over time. Scenarios will be unique to each organization, market, and geography, but there are best practices organizations can use.

- Plausible scenarios should incorporate both worries and vulnerabilities:
    - Worries are specific threats that leaders feel could create catastrophic damage. Worries are informed by past events, near misses, and threats affecting peers within the industry.
    - Vulnerabilities are the known risks and single points of failure. Vulnerabilities are identified during service mapping activities.
- Scenarios need to be plausible, but organizations should be more concerned with the potential impact, as opposed to the likelihood they will occur.
- A formula used to build scenarios is helpful when tailored to IBS:
    - [CAUSE/THREAT] affecting [ACTIVITY/RESOURCE] disrupting [BUSINESS SERVICE] resulting in [IMPACT] for [MARKET/SEGMENT]
- Testing plans need to contain different testing types to ensure that organizations can recover within stated impact tolerances, and testing methods should evolve over time.
- Testing types can include desktop paper-based tests, simulations, live systems, or a combination of these methods.

> Identifying plausible scenarios and testing them allows organizations to validate assumptions and gradually work towards a more resilient organization. Plausible scenarios can help make continuity and response planning seem more real and less abstract. When incorporated into testing plans, plausible scenarios help improve engagement.

Integrate Third-Party Risk Management into Resilience Initiatives

Third-party risk management (TPRM) focuses on identifying and reducing risks relating to the use of third parties. TPRM is considered its own risk discipline, but the growth of dependencies on third-party providers, the potential for concentration risk, as well as intra-organization dependencies means that organizations should consider TPRM as part of any resilience program. Risk management is important because failure to assess third-party risks exposes an organization to supply-chain attacks, data breaches, and reputational damage. You can outsource responsibility but not accountability.

Resilience and operational risk standards and regulations all acknowledge the need to identify critical third parties but vary in the level of scrutiny of controls and mitigations mandated. Organizations must capture the contributions of third parties as part of the delivery of an IBS and should understand the level of risk that a third party introduces if resilience and continuity arrangements are inadequate.

> **Third-party risk management is a form of risk management that focuses on identifying and reducing risks relating to the use of suppliers and other third parties. Organizations must understand the role third parties play in the delivery of their important business services.**

Regulatory Similarities and Differences

All regulations and guidance highlight the need to understand which third parties contribute to the delivery of an IBS or critical operations and the level of risk they potentially introduce; however, regulations differ in how they mitigate these risks.

MAS (Singapore) and the U.S. are fairly prescriptive in outlining actions that should be taken by organizations. This includes using formal agreements to set performance standards, performing periodic monitoring, incorporating requirements during contract negotiations, and developing plans to mitigate loss of a third party. MAS provides very practical requirements for third parties that can also be used by regulated and nonregulated organizations, including:

- Reviewing third-party SLAs and recovery expectations
- Reviewing continuity plans
- Establishing contingency arrangements
- Conducting audits of third parties
- Performing joint testing

In addition to internal controls, the Bank of England is currently examining how supervisory authorities could use their power to ensure appropriate resilience of critical third-party providers, which could include requiring potential critical third parties (CTP) to participate in scenario testing, sector-wide exercises, cyber-resilience testing, and skilled persons reviews of CTPs. Discussions on how much risk can be addressed through mandating internal controls and use of regulation for CTPs are expected to continue.

In Perspective

There are several best practices to better understand third-party risk:

- A service mapping exercise (or a BIA) that includes identification of third parties is non-negotiable. Additionally, organizations need to consider how third parties are used and if using multiple services from a single third party creates a concentration risk. Third-party risk should not be seen as a procurement problem.
- TPRM is a collaborative process with multiple stakeholders. Having a common way of assessing inherent and residual risk across different teams will help build a complete picture of a third party.
- TPRM goes beyond external firms. Organizations also need to examine intragroup and intracompany arrangements that are essential for the delivery of IBS.
- Live by the statement provided by HKMA – "An [organization] should not enter into, or continue, any third party or intragroup arrangements that may weaken the operational resilience of the [organization's] critical operations."

Improve Information and Communication Technology and Cyber Resilience

With an ever-increasing dependence on automation and technology, geopolitical instability, the use of cyber warfare, shortages of information security and technology staff, and challenges preventing and mitigating cyberattacks, the need for resilient information and communication technology (ICT) and cyber resilience cannot be understated.

ICT and cyber resilience are their own disciplines and are pivotal in ensuring disruption does not catastrophically affect markets, customers, or the very survival of an organization. However, the regulatory landscape has been demonstrating signs of convergence between ICT and cyber resilience, operational resilience, business continuity, and third-party risk management. Resilience regulations and guidance documents do not outline every provision required to successfully manage ICT risk, but there are a few key areas that are repeated across resilience-related regulations. Organizations need documented ICT policies (inclusive of cybersecurity) and programs to monitor:

- Cybersecurity controls and measures
- Documented incident management policies
- Priorities based on the level of criticality of data and a systems role in delivering IBS

The last statement shows why regulators are so keen to highlight ICT and cyber requirements in operational resilience and risk guidance. The EU's Digital Operational Resilience Act (DORA) is the primary example of this convergence. It provides requirements around five core areas, including:

- Information and Communication Technology (ICT) risk management
- Reporting of major ICT-related incidents to the competent authorities by financial entities
- Digital operational resilience testing
- Information and intelligence sharing in relation to cyber threats and vulnerabilities
- Measures for the sound management of ICT third-party risk by financial entities.

The ICT risk management provisions in DORA directly align to many operational resilience requirements and seek to create a holistic view of operational risk. These provisions also draw out requirements for complimentary activities, such as risk governance, business continuity policy, and identifying critical operations. All of these provisions seek to create resilience, minimize impact of disruption, and assure operational integrity.

> Digital operational resilience is the ability to build, assure, and review operational integrity from a technological perspective.

Regulatory Similarities and Differences

All regulations and guidance documents highlight the need to identify critical technology and information dependencies and the need to analyze ICT resources during mapping processes. Some regulators, such as OCC guidance in the U.S. and the CBI (Ireland), provide additional guidance.

The U.S. document outlines broad categories to be considered for a cyber risk management process, including requirements on governance, identification of assets and risks, protection and detection of threats, response, recovery, and third-party risk management.

DORA is the outlier and by far provides the most concrete guidance. With a planned full implementation date of January 17, 2025, DORA is hundreds of pages long and lays out numerous requirements for firms in the EU. However, there are practices that are relevant to other geographies and to nonregulated organizations.

In Perspective

There are many ICT and cyber-related best practices that must be considered when building and designing a resilience program, such as:

- Using ICT risk management outputs can greatly improve the quality of dependency mapping activities. For example, having information on the criticality of data and third-party hosting arrangements will help assess the impact of disruption.
- Incident management processes are significant considerations when developing broader response and recovery frameworks. Organizations should work to ensure that response is not considered solely from a technical perspective.
- ICT, cyber threat, and reporting intelligence should feed into the broader resilience program to allow organizations to anticipate and respond to threats more rapidly.
- Hosting arrangements and use of third-party ICT providers can introduce significant concentration risk. Ensure there is a clear understanding of how (and where) key ICT assets are hosted.

Case Study

The Operational Resilience Journey

This is a fictious case study about a firm called Felder, which manufactures various types of medicines, pharmaceuticals, and treatments across 30 global sites. While operational resilience is not mandated in this industry, Felder has been subject to several recent events that have caused it to rethink how it manages operational risk and business continuity.

BACKGROUND

Felder performs research and development activities for each of its major product lines and performs manufacturing. Manufacturing sites are organized around major business lines and areas of focus, which include genetic therapies for rare diseases, plasma therapies, vaccine development, cardiology, and oncology products. Felder relies extensively on third parties for distribution. The company has taken stock of the products and services it provides to customers during previous business-continuity activities.

IDENTIFY BUSINESS SERVICES AND CRITICAL OPERATIONS

During a review of products and services, Felder used the 13 points outlined by UK regulators to assess whether a service could be deemed important and therefore an in-szcope priority. While not a financial firm, Felder considered impact to the patient, as well as the overall health system and if there were products that could serve as substitutes. It had to consider factors outside of financial regulation. For example, patient-health concerns far outweighed other variables. Some of its products do not have market substitutions and are true life savers. The company also had to consider vulnerable customers in determining whether a service was important.

When the dust settled, the management team identified approximately 10 services to map from beginning to end and determine the level of resilience. One of those services is "manufacture and distribute biologic products."

Riskonnect worked with Felder to make sure that the IBS has a designated start point, end point (hand-off to third-party distributor), and could be evidenced by an output (the biologic products themselves).

SET IMPACT TOLERANCE

Felder had to consider several factors in establishing impact tolerance. While the company had not yet performed detailed service mapping, it was able to leverage continuity data to understand the different manufacturing locations and geographic concentration. It worked with the business-line owner and product owners to understand the volumes and capacities for production at each site, which served as baseline metrics to accompany the time metric used in setting impact tolerances. It also worked to understand its customer base, including providers and approximate patient numbers to determine potential impacts of a disruption. Felder pulled financial and revenue data for products associated with its services, including "Manufacture Biologic Products and Prepare for Distribution."

In addition to these quantitative numbers, the team coordinated with the enterprise risk team, which oversees operational risk. They were able to understand impact scales used across the company to assess risk and existing risk-tolerance statements. The team then looked at the top-level impact categories associated with operational resilience, such as impact to markets, impact to customers, and impact to the organization.

As a nonfinancial firm, Felder had to make additional modifications to the way it assessed impact tolerance. Instead of just considering impact to markets, customers, and the organization, it also had to build in additional considerations to determine potential impact to patient safety, which was the overriding concern.

When the team analyzed the data, they were able to create impact tolerances, which included timelines and production capacity (other metrics). For "Manufacture and Distribute Biologic Products" the team proposed to management that the impact tolerance be set at 72 hours not affecting more than 50% of production capacity.

CONDUCT SERVICE MAPPING AND IDENTIFY INTERCONNECTIONS AND DEPENDENCIES

Now that Felder understands its IBS and associated impact tolerances, it can address service mapping. The team coordinated with product and service leaders to understand each IBS value stream, starting with the acquisition of resources to the point the completed product is provided to a third party for distribution – and ultimately delivered to providers and patients.

For "Manufacture and Distribute Biologic Products," the team examined each major production process and looked at resources across major pillars, including technology, information, people, and facilities/equipment. What it found was that there are:Numerous third parties used for requisition of raw materials

- Numerous third parties used for requisition of raw materials
- Three production sites
- Numerous pieces of specialized equipment
- Operational technologies used for manufacturing
- Information technologies used for ERP planning and the processing of information used to meet FDA requirements

The team also identified numerous potential single points of failure, such as ERP systems and third parties. Information was used by the business continuity management (BCM) team to look for manual workarounds and evaluate the effectiveness of continuity planning at each manufacturing site.

IDENTIFY AND PERFORM TESTING OF PLAUSIBLE SCENARIOS

Looking at the outputs from the service mapping exercise, leaders identified several concerns. First, they are worried about the threat of a cyberattack and are particularly concerned with vulnerabilities that may exist in their OT network used for complex manufacturing. This was substantiated through multiple vulnerabilities in the security program, as well as the expertise needed to respond to a disruption.

Felder has a blind spot in understanding the level to which OT and IT networks are air gapped. The company also significantly relied on third parties, particularly the distribution provider. Without the current distribution provider, there are no other contractual arrangements in place to transport and distribute Felder products. Felder was worried about facility dependencies, but since production can occur at three separate locations and capacity is factored into impact tolerance, this is a secondary concern compared to technology and third-party vulnerabilities.

Felder creates a few plausible scenarios around their concerns, including: "cyberattack affecting the OT network required for the manufacture and distribution of biologics products, resulting in health and safety impacts for vulnerable patients."

This plausible scenario (along with others) is examined by the team, which must consider the scenarios to test first, what the most appropriate types of tests will be, and if tests can be matured over time to ensure Felder stays within its impact tolerance. This is integrated into a multiyear testing plan.

INTEGRATE THIRD-PARTY RISK MANAGEMENT INTO RESILIENCE INITIATIVES

Resilience initiatives at Felder helped identify several critical third parties during service mapping. Teams looked at data from BCM initiatives, as well as TPRM information, to holistically look at third-party risk. The team coordinated with TRPM to better understand how inherit risk is determined and the level to which operational risk is considered, which controls various teams are looking for (BC and security play a prominent role), and what actions are taken once residual risk is determined.

The team is able to run a number of high-impact vendors through the model, which identifies a number of gaps. It is unclear what actions should be taken once the level of residual risk is determined. There is also not a great mechanism to determine whether risk should be accepted, mitigated, or transferred. The team identifies many survey and outreach questions that need to be updated based on the resilience initiatives Felder is pursuing.

IMPROVE INFORMATION AND COMMUNICATION TECHNOLOGY AND CYBER RESILIENCE

Based on the concerns around technology, Felder management directs the team to do a deeper dive in the organization's ICT and cybersecurity programs. The programs rely heavily on an outsourced provider, which provides tremendous technical depth. While the technical expertise is clearly present, there are several administrative controls and policies that are lacking. Additionally, the outsourced provider is relatively inexperienced in managing technical remediation with OT environments.

During a review of incident management processes, Felder realizes that technical responses are well-developed but the skillsets of the siloed incident response team creates a situation where technology-related incidents are rarely brought up outside of the IT department. This creates blind spots for management who don't necessarily understand how incident management works or their role in the process.

The team continues third-party analysis into IT infrastructure and service providers. What Felder finds are significant initiatives to improve migration to the cloud but with little thought given to resilience.

When asked about capabilities, team members note that there is redundance between availability zones, but analysis reveals significant geographical concentration risks with little to no availability to restore from backups or snapshots in a different geography. Product managers have repeatedly brought up data locality concerns, but these seem to be secondary cost savings associated with cloud migrations. The team notes these items and factors it into the overall assessment of Felder's resilience and ability to remain within impact tolerances.

Requirements, Regulations, and Best Practices

Australia (APRA) – Operational Risk Management

In July 2022, the Australian Prudential Regulation Authority (APRA) released a draft standard on operational risk. The goal is to introduce minimum standards for managing operational risk, including business continuity and third-party management. Five separate standards will be superseded by the new CPS 230.

KEY REQUIREMENTS

APRA-regulated entities must:

- Manage operational risks and set and maintain appropriate standards.
- Maintain critical operations within tolerance levels through severe disruption.
- Manage risks associated with the use of service providers.
- Identify, assess, and manage risks that may result from inadequate or failed internal processes or systems.
- Prevent disruption to critical operations and adapt processes and systems to operate within tolerance levels.
- Not rely on service providers unless it can ensure that it can continue to meet its prudential obligations in full.

TAKEAWAYS

CPS 230 is expected to commence in July of 2025. It draws from multiple risk disciplines, including outsourcing, business continuity management, and operational risk. Business continuity and outsourcing requirements are integrated into a more holistic operational risk framework. These requirements are similar to other regulations, such as defining critical operations and establishing tolerance levels, and includes business continuity requirements to minimize disruption to critical operations.

RESOURCES

Prudential Standard CPS 230 – Operational Risk Management

AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY

Operational Risk Management

Applicability

- Banks
- Credit unions
- Building societies
- General insurance
- Reinsurance
- Private health insurance
- Superannuation

Status

Implementation to commence in 2025

European Union – Digital Operational Resilience Act

The EU's Digital Operational Resilience Act (DORA) is a requirement that seeks to build ICT and cyber resilience across the financial sector. Originally introduced in 2020, final agreement on the technical requirements was approved in mid-2022. It is unique in that it not only applies to financial institutions but also to critical ICT providers that service the financial sector, such as hosting and cloud providers.

KEY REQUIREMENTS

DORA includes requirements around a few major pillars:

- Implementation of an ICT risk management program
- Requirements on the management, classification, and reporting of ICT-related incidents
- Digital operational resilience testing
- Management of ICT third-party risk
- Oversight of critical third-party service providers
- Information sharing and reporting of cyber threat information and intelligence

TAKEAWAYS

DORA is expansive and has multiple integrations with other regulatory requirements and best practices, spanning operational resilience, business continuity, and IT disaster recovery. A primary goal is to standardize and evolve existing practices with the intent of improving overall operational resilience. Implementing DORA, other operational resilience requirements, and operational risk best practices will require organizations to take a broad, strategic perspective.

RESOURCES

Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector

COUNCIL OF THE EUROPEAN UNION

Digital Operational Resilience Act (DORA)

Applicability

- Financial-sector participants
- Critical third-party service providers

Status

Compliance expected in 2025

Global (Basel) – Principles for Operational Resilience

The Basel Committee's Principles for Operational Resilience build off existing requirements from Basel regarding operational risk management and emphasize the use of existing risk governance structures to manage operational risk with the goal of improving resilience. Similar to other approaches, Basel's Principles for Operational Resilience incorporates previous guidance on outsourcing, business continuity, and risk management.

KEY REQUIREMENTS

Significant requirements from Basel are applicable to large global financials and banks and include:

- Governance
- Operational risk management
- Business continuity planning and testing
- Mapping interconnections and interdependencies
- Third-party dependency management
- Incident management
- ICT (including cybersecurity)

TAKEAWAYS

Basel sees operational resilience as an outcome based on the effective management of operational risk. Since Basel sees resilience as the effect of a well-functioning risk management program, the emphasis it places on the use of existing governance structures is not surprising. Basel also defines the role of business continuity in achieving operational resilience, which provides useful insights for continuity program managers seeking guidance on how to leverage existing continuity-related materials to meet operational resilience objectives.

RESOURCES

Principles for Operational Resilience

BASEL COMMITTEE ON BANKING SUPERVISION

Principles for Operational Resilience

Applicability

- Central banks

Status

Guideline – in effect

Hong Kong SRA (HKMA) - Operational Resilience

The Hong Kong Monetary Authority (HKMA) provides nonstatutory guidelines that authorized institutions should consider when developing an operational resilience framework. These guidelines share practices and terminology with the Basel Committee on Banking Supervision's Principles for Operational Resilience.

KEY REQUIREMENTS

Major provisions outlined by HKMA include:

- Developing an operational resilience framework
- Establishing the role of the board and senior management
- Determining operational resilience parameters
- Identifying critical operations
- Setting tolerances for disruption
- Identifying severe but plausible scenarios
- Mapping interconnections and interdependencies underlying critical operations
- Preparing for and managing risks to critical operations delivery
- Testing ability to deliver critical operations under severe but plausible scenarios
- Responding to and recovering from incidents

TAKEAWAYS

HKMA's guidelines build heavily from other sources and provide a concise list of requirements that are useful to check against an organization's risk framework. The guidelines contain operational risk requirements outlined in Basel, as well as many of the core requirements from PRA/FCA requirements. Since the requirements are broader than those in other documents, it is helpful to review major requirements before examining details of other regulations.

RESOURCES

Supervisory Policy Manual – OR-2 – Operational Resilience

HONG KONG MONETARY AUTHORITY

OR-2 Operational Resilience

Applicability

- Authorized institutions under the HKMA

Status

Nonstatutory guideline - In effect May 2022

Fully implemented in 2023

Ireland (CBI) – Operational Resilience

The Central Bank of Ireland (CBI) provides practical guidance on the implementation of an operational resilience program. It builds off guidance from Basel and the UK's PRA/FCA but has an additional emphasis on planning and response. Similar to HKMA's guideline, it provides a comprehensive look at what goes into establishing an effective resilience program.

KEY REQUIREMENTS

- Governance
- Identification of critical or important business services
- Impact tolerances
- Mapping of interconnections and interdependencies
- ICT and cyber resilience
- Scenario testing
- Business continuity management
- Incident management
- Communications plans
- Lessons learned exercise and continuous improvement

TAKEAWAYS

One of the highlights of the CBI guidance is that it provides a discreet 15-point list outlining what goes into a successful operational resilience program. It also makes that case that business continuity management, incident management, and crisis communications be fully integrated into the resilience framework. Another unique element is the emphasis placed on continual improvement, as evidenced by requirements to conduct a lessons-learned exercise following major events and to establish a culture around learning and continual improvement.

RESOURCES

Cross Industry Guidance on Operational Resilience

CENTRAL BANK OF IRELAND

Cross Industry Guidance on Operational Resilience

Applicability

- Regulated financial-service providers

Status

In effect

Singapore (MAS) – Guidelines on Business Continuity Management

Instead of issuing a separate operational resilience guideline, MAS substantially updated its Business Continuity Management Guidelines. The revised guidelines include both core business continuity requirements and operational resilience requirements, updating language and concepts to align with regulatory trends in other jurisdictions.

KEY REQUIREMENTS

- Critical business services and functions
- Service recovery time objectives
- Dependency mapping
- Concentration risk
- Continuous review and improvement
- Testing
- Audit

TAKEAWAYS

The MAS regulation is the best example of evolving a business continuity approach to address emerging resilience best practices. MAS indicates that business continuity-related activities, such as conducting a business impact analysis, can be used to identify critical services. Similarly, MAS extends concepts like recovery time objectives to apply to services, effectively mimicking concepts such as impact tolerance. MAS is also unique in that it mandates a crisis management structure, inclusive of incident management.

RESOURCES

Business Continuity Management Guidelines

MONETARY AUTHORITY OF SINGAPORE

Business Continuity Management Guidelines

Applicability

- Banks
- Capital markets
- Insurance
- Payment providers

Status

In effect

United Kingdom (PRA/FCA) – Operational Resilience

As the first operational resilience-specific regulation to take effect, the Bank of England's requirements have had an outsized effect and have led to many of the requirements that are being considered or implemented in other regulatory jurisdictions. While the Bank of England acknowledges the inter-relationship between business continuity management, outsourcing, operational risk and operational resilience, the regulation focuses on important business services.

KEY REQUIREMENTS

- Identify important business services
- Set impact tolerances
- Establish strategies, processes, and systems to comply with requirements
- Identify and document resources to delivery IBS (mapping)
- Develop a testing plan, carry out scenario testing, and Document Lessons Learned
- Document a self-assessment
- Maintain an internal and external communications strategy

TAKEAWAYS

Bank of England focuses on how firms identify IBS and remain within their impact tolerances. Bank of England takes a distinctly external approach, focusing on those activities that are likely to affect customers, markets, and organizations to the extent that a disruption could create knock-on effects for market participants. The PRA provides good insight on how operational resilience interacts with other risk disciplines but sees these approaches as complimentary. As Bank of England assesses progress on the first set of requirements (IBS and impact tolerance), we expect to see additional insights that will impact regulations in other jurisdictions.

RESOURCES

FCA Handbook – SYSC 15A Operational resilience

PRA – Statement of Policy - Operational resilience

BANK OF ENGLAND (PRA AND FCA)

Operational Resilience

Applicability

- Banks
- Investment firms
- Building societies
- Insurance
- Payment providers

Status

In effect/enforcement of all requirements to occur in 2025

United States (OCC, Federal Reserve, FDIC) – Sound Practices to Strengthen Operational Resilience

Regulators in the US took a different approach in developing operational resilience guidance. Instead of introducing new regulation, the OCC, Federal Reserve, and the FDIC (the Agency) pulled together best practices from existing regulation to provide guidance to America's largest financial institutions regarding resilience best practices. As such, the guidance provided is not a regulation itself, but a compilation of practices in previously issued regulatory guidance.

KEY REQUIREMENTS

- Governance
- Operational risk management
- Business continuity management
- Third-party risk management
- Scenario analysis
- Secure and resilient information system management
- Surveillance and reporting

TAKEAWAYS

Since the Agency guidance pulls together pre-existing guidance, there is not substantially new information; however, the Agency provides requirements around defining critical operations and setting tolerance for disruption in step with previously established operational risk practices. The exception to this is Appendix A, which introduces sound practices for cyber risk management and incorporates key themes, such as defining critical operations and establishing tolerances.

RESOURCES

Sound Practices to Strengthen Operational Resilience

OCC, FEDERAL RESERVE, AND FDIC

Sound Practices to Strengthen Operational Resilience

Applicability

- Financial institutions for banks greater than $250bn consolidated assets

Status

Sound practices only/ not a regulation

Canada (OSFI) – Operational Resilience and Operational Risk Management

The Office of the Superintendent of Financial Institutions (OSFI) in Canada has updated its operational risk guideline to include tenants of operational resilience regulation found in other jurisdictions. The new requirements will add to previous operational risk regulation and include activities such as identifying critical operations, setting impact tolerances, and mapping dependencies. OSFI has organized requirements around a variety of principles.

KEY REQUIREMENTS

- Operational risk governance
- Operational risk management
  - Framework
  - Risk appetite
  - Tools, monitoring, and reporting
- Operational resilience
  - Identification and mapping of critical operations
  - Tolerances for disruption
  - Scenario testing
- Coordination with other key areas to strengthen resilience

The draft guidance also outlines guidelines for business continuity, disaster recovery, crisis management, change management, technology and cyber risk management, third-party risk management, and data risk management. Each of these areas has its own guidelines and lists of requirements.

TAKEAWAYS

OSFI seeks to unify operational risk and operational resilience practices and has organized its guidance to reflect that objective. The requirements are broad in mandate, particularly when looking at all the ancillary risk disciplines that are referenced. The guideline was published on August 22, 2024. The requirements to maintain operational risk governance and a risk management framework are effective immediately. Operational resilience requirements will be fully enforced September of 2026.

RESOURCES

Operational Resilience and Operational Risk Management

OSFI BSIF

OPERATIONAL RESILIENCE AND OPERATIONAL RISK MANAGEMENT

Applicability

- Federally regulated financial institutions

Status

In effect/enforcement of all requirements to occur in September of 2026

Conclusion

Operational resilience is an emerging and evolving concept. There are numerous opinions on how to leverage best practices while incorporating new practices that help elevate risk and contingency planning to a strategic level. Emerging guidance on operational resilience can be distilled into several key themes that when combined with best practices – in business continuity, IT disaster recovery, cybersecurity, operational risk, and third-party risk management – can greatly aid an organization's ability to anticipate and respond to disruption.

For more on building resilience, check out Riskonnect's Business Continuity & Resilience software solution – or book a meeting with our experts.

BOOK A MEETING →

INTEGRATED RISK MANAGEMENT SOLUTIONS

RISK MANAGEMENT INFORMATION SYSTEM

CLAIMS MANAGEMENT

BILLING

POLICY ADMINISTRATION

HEALTH & SAFETY

THIRD-PARTY RISK MANAGEMENT

ENTERPRISE RISK MANAGEMENT

INTERNAL AUDIT

INTERNAL CONTROLS MANAGEMENT

POLICY MANAGEMENT

COMPLIANCE

PROJECT RISK MANAGEMENT

TECHNOLOGY RISK MANAGEMENT

BUSINESS CONTINUITY & RESILIENCE

ENVIRONMENTAL, SOCIAL & GOVERNANCE

ACTIVE RISK MANAGER

HEALTHCARE RISK & PATIENT SAFETY

ABOUT RISKONNECT

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents use our unique risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia. To learn more, visit riskonnect.com.

CONTACT **770.790.4700** | **PARTNERS@RISKONNECT.COM** | **WWW.RISKONNECT.COM**