

The Operationally Resilient Organization

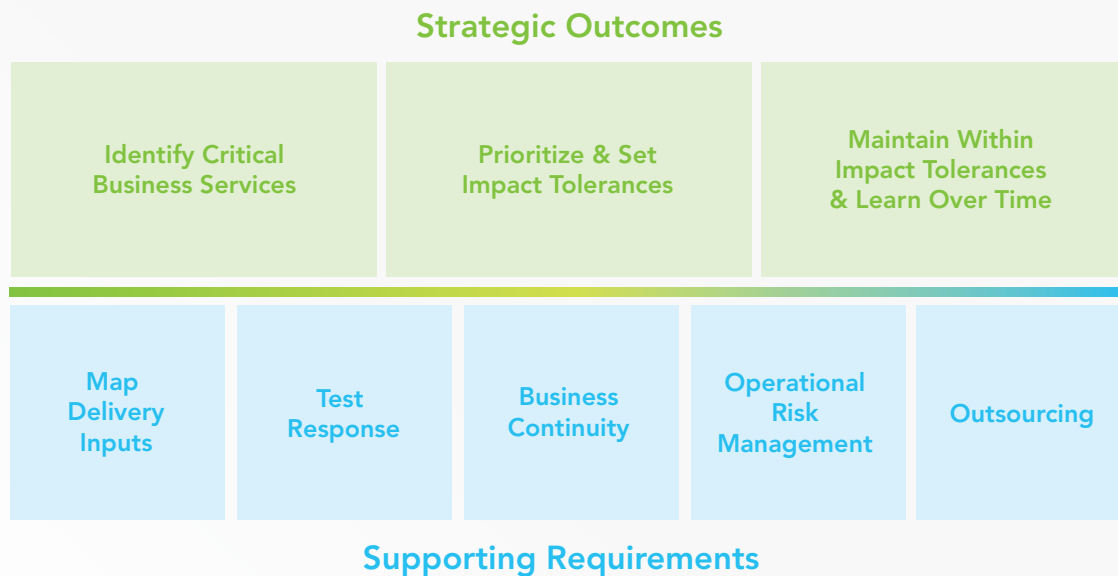


TABLE OF CONTENTS

Critical Elements of a Financial Services Operational Resiliency Program	2
Identify Services	3
Map Resources	4
Set Impact Tolerance	5
Scenario Testing and Validation	6
Response and Communication	6
Incorporating Learning over Time	7
The Operationally Resilient Organization: Call to Action	8
About Fusion	9
Our Platform	9
Fusion's Unique Layered Architectural Approach Adapts With You	10

Critical Elements of a Financial Services Operational Resiliency Program

Guidelines for Implementation



Operational resilience is a significant concern to a broad scope of diverse businesses across the financial industries. Without a firm-wide and systematic approach to operational resilience, these vulnerabilities will drive commercial risk and threaten growth.

The UK regulators have defined operational resilience as the ability of firms and their industry sector(s) as a whole to prevent, adapt, respond, recover, and learn from operational disruptions. This can be broken out into four key practice areas.

Operational Resilience *Protect the firm and your clients.*



Whether creating a program from scratch or growing an established program, leaders must leverage frameworks and methodologies that are agile and resilient – just like the teams they serve.

While the specific activities and processes vary firm to firm, organizations undertaking operational measures to enhance resiliency follow a common set of steps:

Initial Activities for Operational Resilience

1

Identify Services

Organizations need to identify and document the critical or important business services which have considerable systemic impact internally and externally.



2

Map Resources

Service dependencies need to be mapped using processes as the center point – critical resources are systematically brought to the surface for analysis and consideration.



3

Set Impact Tolerance(s)

Impact tolerances are set (based on specific impact categories) leveraging the most critical data/information fed from the mapped resources and continuous monitoring activities.



4

Scenario Testing and Validation

Organizations must test their ability to remain within impact tolerance for each critical or important service – this helps to validate the confidence level on the resilience of services.



5

Response and Communication

Impact tolerance testing and analysis should focus on the response and recovery actions organizations would take to continue the delivery of critical or important business services.



Achieving a mature and robust operational resiliency program requires a broad, integrated range of activities connected to governance, risk management, and compliance. These elements make up the foundation of building maturity within the organization's approach to managing risk and achieving resilience.



Identify Services

Identification and documentation of what services are critical is the first step. Every organization will differ in their approach and the consensus needed to arrive at a list of critical services. This includes thorough documentation of the services and reasoning on its criticality and impact on the business.

A critical business services approach is an effective way to prioritize improvements to systems and processes and drive prone to failure, anticipated costs of financial failure, or the cost of upgrade against available budget. Such considerations may be inconsistent with an outcome centered around continuity of business services. Looking at systems and processes based on the business services they support brings more transparency to improve the quality of decision making, thereby improving resilience.

Operationally resilient business services in organizations reinforces resilient economic functions. Financial systems are resilient if their economic functions can continue to operate during disruptive incidents. Resilience of the financial system depends on both individual organizations and the ways in which their services are interconnected with other organizations.

The benefits of continuity of critical business services include better customer outcomes and insight across departmentalized silos within the organization. On the other hand, for larger organizations with more complex business models and third-party relationships, identifying and documenting critical business services and accountabilities is complex, time-consuming, disruptive, and disproportionately expensive.

In the financial services industry, a critical business service can be identified as a service that, if disrupted, would be most likely to give rise to insupportable levels of loss to consumers or market integrity. This includes services that provide significant exposure to:

- ① Harm to customers/market participants [includes policyholder protection and market integrity],
- ② Safety and soundness of the firm, and
- ③ Systemic financial instability

A critical business service will be identifiable as a separate service and not a collection of services, and the users of the service need to be identifiable, so that any potential impact of disruption, whether internally detrimental or externally harmful, are clear. These include, but are not limited to, retail customers, market participants, and business consumers.

The potential impact on the organization itself that could harm customers/market participants, compromise the safety and soundness of the organization or impair systemic financial stability includes, but is not limited to:

- > Impact on the organization's finances and potentially the organization's continuity
- > The potential impact on the stability and resilience of the financial system and economy overall
- > Reputational damage with potential to give rise to a trickle-down effect to the consumer economy
- > Potential of legal or regulatory action
- > The potential to significantly disrupt the consumer economy could give rise to a trickle-down effect for other market participants

For example, while regulators may only be concerned with operational or systematic impact, an organization will be concerned about reputational and financial impact.

The identification is simply deciding which of your services are deemed "critical" or "important." Once you've done that, you need to begin mapping the processes.

Map Resources

To have a complete view of resilience, organizations need to map the people, processes, technology, facilities, third parties, and information needed to carry out the identified critical business services. Resources for these critical identification.

Organizations are to map the resources that deliver essential business services to develop a clear picture of how best to reinforce and achieve operational resilience. This enables the organization to map exposures in the delivery appropriately. Vulnerabilities may include lack of substitutability, high complexity, single points of failure, concentration risk, dependencies on third parties, and matters outside of an organization's control.

An operationally resilient organization will put into place a comprehensive mapping of the systems, processes, information, relationships, and transactions that reinforce their business decisions.

Mapping all of the integrated dependencies that support a critical business service allows the organization to test and identify the state of their mitigation plans or contingencies (acceptable or unacceptable), and understand – specifically – where investment decisions need to be made to stay within service-level impact tolerances and the corporate risk appetite.

Understanding vulnerabilities with a service provides a contextual perspective that allows the organization to consider alternatives to the way they deliver business services. Centering attention on critical business services and possible disruption allows board members and senior managers to make better informed strategic decisions. They can then move on to establishing impact tolerance levels to understand what levels of disruption are acceptable.



Set Impact Tolerance

Disruption to business services needs to be managed proactively. Disruption is inevitable and setting impact tolerances is a tool for continuity planning and discovery purposes. Impact tolerance is understood to be an organization's tolerance for severe but plausible disruption to a particular important business service and is expressed by referring to specific outcomes and metrics. Impact tolerances ensure that boards and senior management consider how to appropriately respond when a disruptive service-level event occurs and inform where to focus and invest to safeguard against catastrophic impacts both internally and externally. It is often characterized by specific outcomes and metrics, which include the maximum tolerable duration and volume of disruption.

Impact tolerance is related to, but differentiates itself from, risk appetite. The difference is that impact tolerance assumes risk has materialized and may go beyond an organization's timeline for recovery. Impact tolerance is also different from, but again related to, business impact analysis as it is determined with reference to public interests of regulators in reducing damage to consumers and market integrity. For example, in a large company, a financial loss of \$20 million would exceed an organization's risk appetite and have an impact on financial performance, but it may not exceed the absolute risk tolerance levels set via the qualifying economic and systematic criteria.

Impact tolerance statements should cover severe but plausible scenarios, whereas risk appetite statements and recovery time objectives typically cover low tolerances for disruption and an assumed ability to resolve the situation quickly through pre-planned measures.

When setting impact tolerances, organizations are to consider factors which may lead to disruptive activity in critical business services, defining both the duration of the disruption and the quantitative volume associated with the disruption.

Organizations need to set impact tolerances with consideration given to the potential damage that could be caused to:

- ① Customers/market participants
- ② Safety and soundness of the organisation, and
- ③ Systemic financial stability of the external ecosystem to meet the expectation of regulators in addition to brand and financial impacts core to any thriving business institution.

There are a number of metrics organizations can use for impact tolerance that can either be combined or used alone. These help to set the "business-as-usual" baseline to begin identifying severe but plausible disruptions. Measurement details include, but are not limited to:

- > The number and type of consumers affected
- > Financial loss to consumers
- > Financial loss to the organization that could have ripple effects on the consumer, and the overall financial system and markets
- > Potential reputational damage that impacts market integrity and consumer confidence
- > Risk spreading throughout the business to other key internal or external business services
- > Loss of service access for consumers and inability to repair vulnerable market offerings
- > Loss of critical data and exposure of sensitive information
- > Downtime in outsourced services and relationships

Duration-based metrics specify how long a particular business service can remain disrupted for a period of time, while volume-based metrics specify the percentage of normal operating capacity.

Impact tolerance provides the organization with a critical planning tool that defines boundaries for critical business services to remain within, even during severe but plausible scenarios. Delivering operational resiliency requires that organizations take decisive, efficient, and effective action.



Scenario Testing and Validation

Organizations need to test their ability to remain within impact tolerance for each of their critical business services in the event of a severe disruption. At the onset, this exercise helps to substantiate and prove the proposed impact tolerances.

Moreover, this validates their confidence level on the resilience of critical business services, as well as identify where they might need to act to increase operational resilience. In carrying out the scenario testing, firms are to identify an appropriate range of adverse circumstances, severity and duration relevant to its business and risk profile.

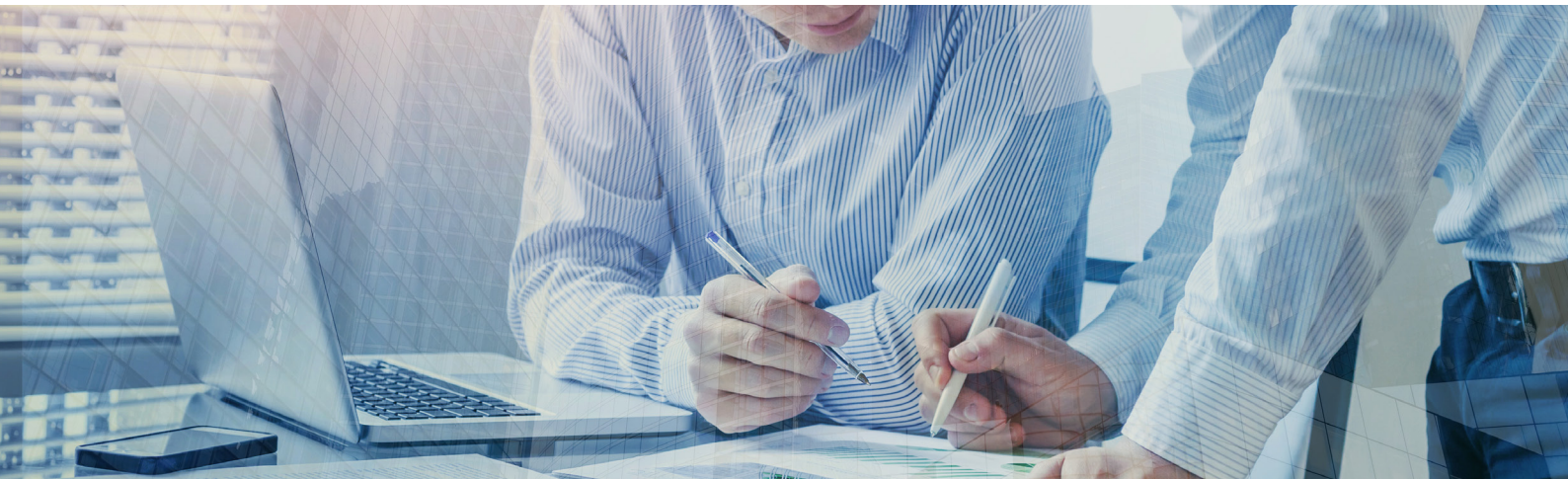
Impact tolerance assumes a disruption has occurred and scenario testing the ability to stay within impact tolerances should not anchor all of their focus on preventing disruptive incidents. Testing includes focus on the response and recovery actions organizations would take to continue the delivery of critical business services. It is important to note that in some cases organizations should consider taking the business service and its systems completely offline.

Organizations need to be able to explain the level of resiliency they built by justifying the severity of scenarios in which they would be able to resume the delivery of a critical business service within their impact tolerance. Organizations are to consider the following:

- > Loss or manipulation of data
- > Unavailability of third-party service providers
- > Disruption to market participants
- > Loss of technology

Lessons learned from exercises are also important as continuous improvements to operational resilience. It requires organizations to learn from experience as their operations and technology changes and their approach matures over time.

Deficiencies, whether identified through scenario testing or through experience, are to be addressed as a matter of priority.



Response and Communication

Fast communications play a critical role in mitigating loss and exposure in times of operational disruption. It is important that organization's internal policies include an effective communications plan, even for external parties such as regulators, the news media, and consumers. Efficient communications help an organization act quickly and effectively to reduce potential damage precipitated by disruptions by providing clear and prompt communications.

A mature communications plan will require both internal and external components. An internal communications plan includes escalation paths the organization can use to manage communications during an incident and identify appropriate decision makers. An external communications plan includes advice and warnings to relevant stakeholders.

Communication plans also need to extend to the organizations third-party relationships. They are not just internal to the organization but require coordination and communication for response across the interdependency of third-party services.

Incorporating Learning Over Time

Requirements relating to an organization's governance of operational resiliency are in abundance.

Initial Program Iteration

SERVICE IDENTIFICATION

Identification of critical or important services.

RESOURCE MAPPING

Mapping of resources to critical or important services.

IMPACT TOLERANCES

First pass at setting defensible impact tolerances.

SCENARIO TESTING

Validation of impact tolerance and current state of service resiliency.

RESPONSE/ COMMUNICATION

Investment decisions to improve current state of service recovery.



REGULAR CHECKPOINT

Health check on methodology to establish realistic impact tolerances.

VALIDATION CHECKPOINT

Validation and challenge of impact tolerances that have been set and current state of service resiliency.

ACTIONABLE CHECKPOINT

How do we need to adjust our current contingency strategies to align with services?

The board and senior management of the organization has to be sufficiently engaged in setting effective standards for operational resilience. Senior management needs sufficient time to establish the business and risk strategies and the management of the main risks relevant to operational resilience.

It is also important for organizations to be able to demonstrate to the relevant supervisory authority that they are meeting their responsibilities in respect of operational resilience. Therefore, it is imperative for organizations to develop a self-assessment document which includes:

- > Identification of critical business services
- > Mapping of dependencies/resources to critical business services
- > Identification of vulnerabilities to critical business services
- > Scenario and stress testing
- > Communication plans
- > Lessons learned exercises

The organization's management and governance bodies need to review this self-assessment document on a regular basis. Self-assessment and the methodologies used to create the document need to be created with proportionality in mind.

The Operationally Resilient Organization

Call to Action

Crisis Management

Disaster Recovery

Business Continuity

Third Party Management

Risk Management

IDENTIFY CRITICAL SERVICES

Detail your business services and identify the critical ones with impact to the customer and the economy.

MAP CRITICAL SERVICES

Understand the dependencies within critical services (process, people, sites, systems, third parties, etc.)

SET IMPACT TOLERANCES

Set thresholds for the maximum impact your business is able to withstand. Set objectives to maintain within those standards.

PLAN FOR SEVERE BUT PLAUSIBLE

Ensure the business has the proper plans to accommodate severe but plausible scenarios.

TEST SCENARIOS

Test your response under realistic conditions.

LEARN AND PIVOT

Uncover gaps and remediate for the future.

Managing operational risks in silos leads the organization to inevitable failure and disruption. Decentralized and disconnected systems catch the organization off guard to emerging risk. The complexity of business and intricacy and interconnectedness of risk requires an integrated, efficient, and agile approach. It is necessary for a distributed and disrupted business to have a strategic approach to operational risk and disruption, enabled with an integrated information and technology architecture via a single pane of glass. The organization needs complete situational awareness and understanding of risk across sites, third-party relationships, processes, information, and systems to see the big picture of risk and any potential disruption.

UK regulators have been direct with their expectations in that firms need to look at what would pose a risk to the stability of the UK financial sector (financial stability) or a firm's safety and soundness. For many firms, they recognize that this will mean a shift away from thinking about the resilience of individual systems and resources and a shift towards considering the services that are provided to users (identifying important business services).

Prevention isn't always effective and may present undesired consequences such as missed competitive opportunity, obstacles to innovation, and slowed progress toward key strategic objectives. Organizations are developing the agility to look for patterns and relationships between risks to foretell risk events, identify upsets in business process, and contain and reduce the impact of events when they occur, including those that occur external to the organization, with outsourced providers of key services.

Organizations have a complicated web of operational risk, third-party relationships, and business continuity management programs. They naturally try to react and put out fires, addressing risk and compliance in solitary approaches, but they really need to step back and think strategically and not tactically. They need to look to how they can strategically address risks and operational disruption across the organization.

Developing a coherent strategy and technology architecture to link and measure potential risks and disruptions to strategic objectives and monitor performance against those objectives is critical. The outcome of this is improved decision-making, better return on investment across the business, improved profitability, and a better customer experience.

Successful operational resiliency requires the organization to provide an integrated process and technology architecture to identify, manage, and monitor risk and disruption to capture changes in the organization's risk profile from internal and external events as they occur internal to the organization and across its critical third-party relationships. Mature operational resiliency is a seamless part of governance and operations. It requires the organization to take a holistic view of risk, not an unattached layer of oversight. It also involves a bottom-up participation where departments and functions at all levels of the organization identify and monitor uncertainty and the impact of risk and possible disruption. Organizations striving to increase operational resiliency maturity in their organization become more:

➤ **Agile**

Stakeholders and senior management desire that the organization be fast, but agility isn't useful to the organization if it is headed in a direction it shouldn't be. Agility allows the organization to be confident in its ability to stay on course while facing emerging risk and disruption.

➤ **Efficient**

Organizations striving to improve operational resiliency capabilities and maturity need to rid the organization of unnecessary waste and misallocation of resources and redundancy brought about by siloed processes and systems. This is delivered through sound governance and management of operational resilience in a technology platform that integrates the components of operational risk, disaster recovery, and business continuity management.

➤ **Effective**

Effectively managing emerging risk and disruption is easier said than done.

An ad hoc approach means that current risk management processes are outdated, scattered throughout the organization, and lack consistency – creating a confusing nightmare to manage. Organizations need to gain a complete, contextual understanding of emerging risks across the organization that could prove to be disruptive to critical business services and implement a holistic approach to operational risk, disaster recovery, and business continuity management that is delivered through an integrated approach.

The transformation of a more streamlined, optimized approach can position organizations and management teams to address organizational challenges in a prudent and efficient manner.

About Fusion

We are more than a business continuity and risk management company. We are an innovative, forward-looking community with deep experience in the industry. At Fusion, our focus is providing solutions. That means we partner with you to solve problems and create the best fit for your program's needs.

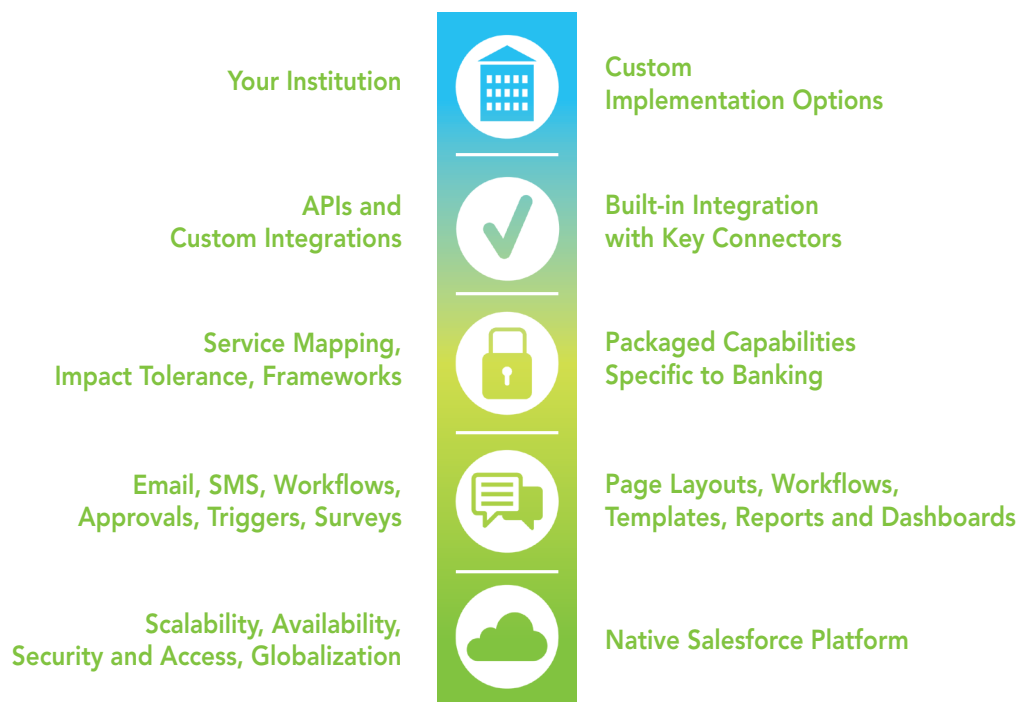
Fusion for Financial Services leverages Fusion's proven, award-winning risk and resilience platform adopted by some of the world's most respected companies, helping boards and executive teams across the globe protect and scale their brands.

Our Platform

Every program is different. Fusion offers a flexible set of tools that can be tailored to your program. Whether you're managing an entire risk database or a small business continuity program, Fusion can be configured to your needs.

- Improve visibility through impactful analytics
- Increase company engagement through automation
- Manage and control your program with visuals and dashboards

Fusion's Unique Layered Architectural Approach Adapts With You



About the Authors

Rich Cooper, Principal-Financial Services

Rich Cooper is the Principal of Fusion's Financial Services practice. Rich leads Fusion's operational resilience global working groups, teaming with the worldwide community of leaders developing best practices, driving innovation across the industry, and designing new solutions that solve the unique needs of financial services organizations.

In his time at Fusion, Rich has consulted with leading financial institutions in the US and Europe across the critical disciplines of operational resilience, cyber, and non-financial risk management, risk data and infrastructure, crisis management, disaster recovery, business continuity, program governance and operating model innovation.

Rich has more than twenty years' experience in the business continuity and risk management community, with experience as practitioner, executive leader, and currently, leader in the solution provider space. Prior to joining Fusion, Rich founded Arbor Continuity Inc. after spending 12 successful years at Business Protection Systems International (BPSI), where he held various executive, service, and sales roles including company President. Before joining BPSI, Richard was a founding partner and CEO of the Packing House Inc. a leading document management company that was ultimately acquired by Iron Mountain Inc.

Rich holds MBCI certification from the Business Continuity Institute.

Paula Fontana, Director, Product Marketing

Paula Fontana leads innovation and product marketing at Fusion Risk Management, a global provider of risk, crisis, supplier, and business continuity management solutions. With over 20 years of experience with startups and large, multinational companies across a broad set of verticals, Paula works with customers and innovation teams to examine and re-engineer the fundamentals of business processes, driving new impact and growth, and building thriving, resilient organizations in the process.

Paula's professional experience includes global leadership roles in innovation, design, development, operations, and delivery at Follett Corporation, Wiley Education Services, LexisNexis, United Airlines, and TransUnion as well as startup organizations in supplier risk management, media, and health care.

*To learn more about
how Fusion can help
your program, visit
fusionrm.com/demo.*



Fusionrm.com
Choose Success. Choose Fusion.