WHITE PAPER

Davies

Operational Resilience

davies-group.com/consulting

in Davies Consulting

Contents

Understanding the risks

Operational Resilience is defined as an organisation's ability to withstand and recover from disruptive events while maintaining continuous business operations. Operational Resilience can be built on existing practices of disaster recovery (DR) and business continuity planning (BCP). However, achieving Operational Resilience requires the whole organisation to play a part by:

- **Focusing on all critical business functions**
- **Identifying key dependencies and interconnectedness between systems, people, processes, and third-party suppliers**
- **Testing scenarios that simulate real-world disruptions**
- **Encouraging a culture of continuous improvement and learning**
- **Establishing clear incident response roles and responsibilities**
- **Building redundancy and diversity into critical systems to minimise single points of failure**

Furthermore, businesses must continually monitor their Operational Resilience plans and procedures, keeping them up-to-date and effective in the face of changing circumstances and emerging threats. It also requires senior executives to buy into and embrace the importance of Operational Resilience, prioritising it to guarantee customer trust, prevent brand damage, protect from financial losses, and comply with regulations.

What are the potential threats to your business?

In recent years the context surrounding Operational Resilience has shifted. Many businesses now have maturing hybrid working capabilities and this change has brought new own operational risks. Increased use of Cloud technology has increased business reliance on off-site data storage and systems, and consumer reliance on digital services has increased as well. The biggest threat to Operational Resilience is now a **cyber attack**.

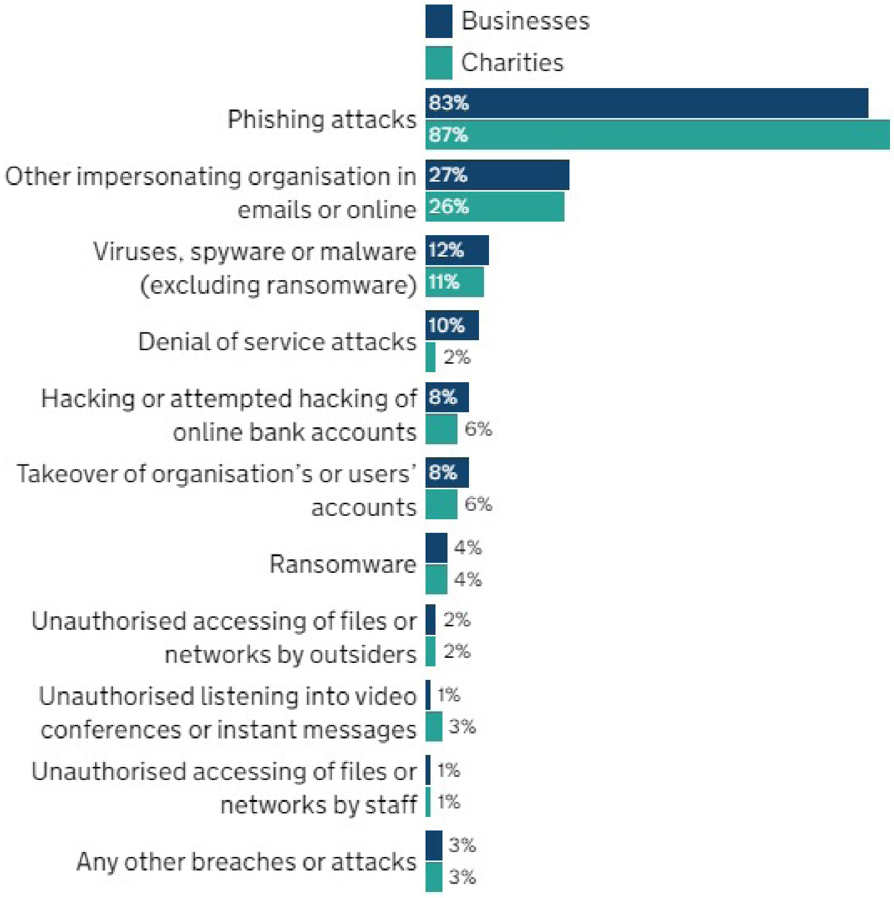
Consumers and regulators are also more sensitive to service disruptions caused by lack of Operational Resilience. There is a greater expectation that service providers take all necessary steps to secure their systems and protect against cyber threats.

As a result, businesses have become focussed on protecting against cyber security threats, but this has meant a reduced ability to protect against and respond to physical disruptions.

To best protect your business, it's important to understand the biggest threats to business continuity, such as:

1. Cyber security attacks

Cyber attacks can cause disruption to critical IT system and compromise the confidentiality of its data. The biggest cyber security threats include hacking, phishing, and malware which can compromise data and systems, causing business disruption and financial loss:



Source: Cyber Security Breaches Survey 2022

- Phishing involves sending emails or other messages claiming to be from a reputable source, to get the recipient to reveal sensitive information that is then used to compromise the individual or organisation

- Malware is software designed to infiltrate and gain access to computer systems. Malware can be deployed as viruses, Trojan horse attacks and ransomware

- Denial of Service (DoS) attacks are designed to overload a system with traffic making it unavailable to carry out its normal operations

- Insider threats are carried out from individuals from within an organisation. These can be accidental or deliberate actions to sabotage, steal or leak sensitive data

In 2020, both Redcar & Cleveland and Hackney councils were hit by ransomware attacks, shutting down key local services for

1 month

In 2017 a ransomware attack halted production for pharmaceutical giant Merck, causing

$870m

in damage

In 2021, Conti extorted at least

$180m

Cost of Ransomware expected to exceed

$365Bn by 2040

(estimated to be $20Bn in 2022)

Global Cybercrime Damage Costs estimate in 2022

$6Tn a year

($190k a second)

Colonial Pipeline paid ransom of

$4.4m

2. **System failures**
   Network outages, hardware failures, software bugs can all cause downtime to IT systems and disrupt services

3. **Third party service provider outages**
   There is always increased risk when you are not in direct control of a service. Third-party providers deliver a myriad of services and outages will affect the ability of an organisation to deliver key business functions

4. **Natural disasters**
   Damage to physical infrastructure affects both organisations and the third-party providers causing disruption to operations. The same damage can impact the ability of employees to carry out their work

5. **Human error**
   This is particularly damaging when processes do not exist or are not well defined

6. **Supply chain disruption**
   Delays, or shortages of materials can impact the ability to provide products and services

Threats will continue to evolve, as technology and business operating models develop. Therefore, to act as quickly and effectively as possible, you need to assess the threat landscape regularly and adapt plans to best practice, incorporate employee training and create incident response plans accordingly.

It is essential for robust disaster recovery and business continuity and that your third-party providers, suppliers, and partners are also ensuring they have Operational Resilience procedures and plans in place.

While technology can provide some level of security, companies must test their overall resilience through:

- **DR and BCP**
- **Critical incident scenario modelling**
- **Verification of third-party providers having implemented strong security measures**
- **Verification of third-party providers having established contingency plans in case of disruptions**

What is the regulators' approach to making businesses operationally resilient?

The regulatory landscape is ever changing as regulators grapple with developing circumstances and consumer needs. In the UK, regulators are focused on establishing a regulatory framework to help businesses measure and adapt their Operational Resilience capabilities. While different industries and sectors are governed by their own regulations and best practices, critical third parties are likely to fall under these regulations.

Operational Resilience Framework

In March 2022, following a period of review, the Bank of England, FCA and Prudential Regulation Authority (PRA) announced a new Operational Resilience Framework for firms stating:

This framework sets out guidelines to help businesses identify important services, set impact tolerances, map and test interdependencies, and develop response and recovery plans. **A deadline of March 2025** has been set for businesses to have assessed and developed their scenario testing capabilities to mitigate severe impacts on key client-facing services.

These regulations will continue to evolve, with further guidance proposed on outsourcing and third-party risk management as regulators recognise the increasing reliance on third-party providers for uninterrupted delivery of important business services.

> Ensuring the UK financial sector is operationally resilient is important for consumers, firms, and financial markets. Operational disruptions can cause wide-reaching harm to consumers and pose a risk to market integrity, threaten the viability of firms and cause instability in the financial system.

Regulations outside the UK

Other regulatory bodies outside the UK are also looking to develop and expand their regulations around Operational Resilience. In the EU, the **Digital Operational Resilience Act (DORA)** refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring. The US prefers a more guideline centred approach, using existing risk management rules to set individual organisational standards around resilience.

Businesses must also comply with data protection laws such as **GDPR in the EU**, which requires businesses to take appropriate technical and organisational measures to protect personal data. Firms may also be contractually obligated to protect their customers' data and to maintain a certain level of Operational Resilience. **If a business fails to meet these obligations they face sanctions, fines or licence revocation that can severely limit their operations.**

> Alongside substantial fines, failing to comply with industry compliance best practice and national or international regulatory standards can lead to time-consuming audits or investigations and open your business up to liability action from consumers and business partners.

What are the consequences of a critical incident?

In the face of increased public and regulatory expectations, businesses must do more to secure their Operational Resilience and protect against threats. Even if your business or industry is not heavily regulated, poor Operational Resilience has the potential to harm your business financially, reputationally, and more.

Businesses that ignore these risks or do not adequately implement an Operational Resilience plan risk their long-term survival.

Financial risks

The financial risks of business disruption are perhaps the most easily quantifiable for organisations and can include everything from:

- Potential regulatory fines and non-compliance sanctions
- Revenue damage caused by the interruption of services, system downtime, and delays
- Loss of revenue as customers take business elsewhere
- Increased operational costs such as new security measures, data recovery efforts, and repairs to assets
- Longer SLAs and operational cost to maintain workaround processes whilst the business recovers
- Increased insurance premiums

Reputational risks

Reputational risks associated with lower consumer confidence stemming from a lack of Operational Resilience are perhaps less easily measured. Reputational risks include:

- Brand damage leading to lack of consumer trust and loss of market reach
- Negative media coverage impacting customer numbers, revenue, and morale
- Reputational contagion affecting associated businesses and individuals, such as partners, contractors, suppliers, and customers

Human capital risks

The most underestimated risk factor is the damage operational inefficiencies and lack of resilience can have on your employees. Higher workloads and a loss of confidence can cause:

- Increased levels of stress and burnout leading to employee fatigue
- Reduced efficiency and productivity
- Increased turnover of crucial staff
- Widening skills gaps within your organisation
- A difficulty in attracting new high-quality talent to your organisation

The costs of complacency and the lasting impact of ignoring risk

In April 2018, TSB experienced a series of severe disruptive incidents when the bank attempted to migrate its customers from a legacy IT system to a new platform. The migration was designed to reduce costs and improve customer service, but it went wrong, causing significant disruption for TSB customers.

In November 2022, the FCA fined TSB £48 million, one of the largest ever imposed, for its role in the IT failures. The FCA found that TSB had failed to take appropriate measures to manage the migration and had not properly tested the new platform before launching it.

Crucially the IT failures were caused by an overall lack of Operational Resilience and a failure to manage third party IT providers correctly. While the size of the fine is what hit the headlines, TSB is far from alone.

$4.35 Million | the average cost of a data breach for a company

Cost of Ransomware expected to exceed $365Bn by 2040 (estimated to be $20Bn in 2022); Global Cybercrime Damage Costs estimate in 2022 $6 Trillion USD a Year = $190k a second.

Big names like British Airways, Equifax and Marriott Hotels have all experienced severe data breaches that have led to financial losses, fines, and reputational damage. Most recently the Royal Mail suffered a ransomware incident that threatened to expose customer data and led to a complete inability to ship international parcels.

Ignoring the risks and failing to maintain Operational Resilience can have significant negative impacts on business continuity. Complacency could have huge long-term financial impacts beyond mere business disruption. Regulatory sanctions for non-compliance can be costly and erode consumer trust. Cyber attacks can leave your IT infrastructure in need of significant security upgrades, and pressure on employee capacity can mean increased staffing costs.

Being prepared with continuous planning for severe disruptive events is becoming part of the fabric of an organisation's risk management. **The 'do nothing' approach is no longer an option with the myriad of impacts that will result from a critical business disruption or outage.**

Prevent and mitigate critical incidents

In January 2023, **23% of UK businesses** reported that they were unable to operate fully due to Operational Resilience failures such as supply chain disruption, system failures, third party outages and cyber attacks.

Putting measures in place to prevent critical incidents from occurring, to ensure your organisation is protected, and to be able to mitigate any risks that may arise is more important than ever to ensure the ongoing delivery of important business services.

How are businesses dealing with business continuity today?

For many businesses the focus of Operational Resilience is still around traditional Business Continuity Plans. This traditional view of how to mitigate and prevent critical incidents is often limited to a small number of major incidents but not on critical customer facing services.

A more proactive Operational Resilience strategy involves taking proactive measures to prevent and mitigate material harm. While businesses are typically able to react to incidents well – they know the escalation path and who needs to be consulted and informed – prevention and mitigation means there should be no surprises and all possible severe disruptions should have been pre-considered and realistic workarounds and mitigations planned.

More mature organisations are developing an integrated set of Operational Resilience capabilities and “playbooks” that help them predict potential problems and respond to critical incidents faster and more efficiently. These capabilities ensure a comprehensive approach that minimises the impact of incidents and ensures continuity of their operations.

Four questions to consider when reviewing your Operational Resilience preparedness

Before you engage in developing your Operational Resilience strategy and plan you need to address four key concerns to establish the organisation's maturity:

1. What is important to your clients?

Under the new FCA regulations around Operational Resilience, important business services are defined through the lens of the client. Harm is caused to clients in several ways when disruption occurs to your important business services:

- Being unable to provide essential services to your clients can lead to financial losses and reputational damage for those clients due to delayed or cancelled services. **They may also lose the trust of their customers, who may take their business elsewhere.**

- **The economic ripple effect of widespread disruption.** As each client business begins to suffer delays financial and reputational losses increase, ultimately affecting the wider economy.

- Falling short of regulatory standards can result in penalties and fines and this can have a knock-on effect to your clients. **Causing a loss of trust, reduction in the services provided and ultimately a loss of business.**

Impact tolerances refer to the level of disruption or harm that a firm can accept before it begins to cause its clients intolerable harm. Knowing these tolerances means firms can take a more strategic risk-based approach to managing disruptions and improving their Operational Resilience. You can then decide how to prioritise investments, focus on prevention, improve incident responses, and enhance communications with clients and stakeholders.

After defining important business services and impact tolerances, it is critical to then map the resources (people, volumes and metrics, technology, facilities, third parties) used to provide these products or services. Dependencies and gaps should also be mapped so you can take appropriate steps against potential risks or threats and create contingency plans to ensure continued delivery of services in the event of disruption.

2. Is your culture in the right place?

Operational Resilience should be an integral part of your workplace culture and be embedded within your Enterprise Governance, Risk and Compliance framework. To do so there needs to be an understanding that resilience isn't a one and done exercise. It is a constant cycle that continuously feeds information to relevant teams and individuals.

Risk is an organism that moves and shifts dependant on internal and external factors. Operational leaders need to be horizon scanning, theorising on additional or emerging risks that could have a critical impact to their business. These should all live within the enterprise risk register.

Another reason for embedding Operational Resilience into your culture is that it cannot be achieved by a small subset of the employee base. The ultimate owner of Operational Resilience will be the Chief Risk Officer (CRO). However, resilience needs to be owned by an entire organisation, feeding into a centralised vision and strategy of managing risk. Without collaboration, you will create a disjointed approach.

Resilience must be a part of the entire employee lifecycle; being part of the conversation from recruitment and onboarding through to training and professional development objectives.

For roles where Operational Resilience is a factor you need to be selecting people with the right understanding and skills. Use skills matrices to evaluate the expertise your current workforce has, determine any Operational Resilience or business services skills gaps and set interview questions to select for required skills.

Training around Operational Resilience should be focussed on elevating every member of your organisations understanding and knowledge. And senior management should have risk objectives to ensure everyone is taking resilience seriously and working towards one common goal. The most operationally resilient businesses will have all employees culturally aligned.

3. Are you scenario testing?

A key aspect of Operational Resilience is robust scenario testing. This important tool enables firms to assess their Operational Resilience, particularly in relation to disruption to their critical services. Scenario testing involves simulating a range of severe, but plausible potential events that could impact a firm's operation and assessing its ability to respond and recover within defined impact tolerances.

This type of testing can help by:

- Identifying **vulnerabilities and highlight areas** that might be most exposed to risk.
- Outlining the steps needed to **mitigate the impact and prioritise investments** accordingly.
- Identifying areas that need to be **improved and refined** to provide a better, faster response.

Scenario testing is now mandated by the Financial Conduct Authority's new Operational Resilience rules. Firms are required to demonstrate they can continue to operate their important services in the event of disruption. First and foremost, testing is conducted to assess your Operational Resilience impact tolerances and your ability to remain within these thresholds.

When simulating plausible real-world scenarios of varying levels of severity, you need to be clear that all your processes have been mapped against risk factors such as people, technology, third party providers, and location. Scenario testing and exercising can also be used to test the effectiveness of any workaround processes and plans as well.

Ongoing testing should be part of your overall Governance, Risk and Compliance strategy. The results of a regular, annual cycle of Operational Resilience scenario testing can then be fed through these structures, improving the effectiveness of your Operational Resilience planning by giving the board visibility and accountability for any improvements that need to be made and the ability to prioritise business funding to address any gaps.

A SecOps (Security Operations) team plays a critical role in assessing and updating the business on the threat landscape. They play a critical role in delivering Operational Resilience to an organisation by implementing and managing security measures that ensure the continuous operation of critical business functions, systems, and data. Some of the ways SecOps teams help deliver Operational Resilience include:

- Identifying **system and network vulnerabilities**
- Responding to **security incidents**
- **Maintaining compliance** to laws and regulations
- Implementing **security controls**

4. Do you understand your Critical Third Parties (CTP)?

Third parties often play a significant part in the delivery of products and services, so disruption to their services can have a knock-on effect to the firm's operations. This could include third parties that provide key infrastructure (cloud computing) and supporting services, such as IT systems, payment processing or entire data centres.

The financial services industry is becoming so reliant on critical third parties to supply key functions and services that the Government issued a specific policy statement in June 2022 to address these risks:

> If many firms rely on the same third party, the failure or disruption of this 'critical' third party could threaten the stability of, or confidence in, the financial system of the United Kingdom.
> HM Treasury, Policy Statement: Critical third parties to the finance sector

CTP will also fall under the FCA's new guidelines for Operational Resilience. A proposed Financial Services and Markets Bill announced in an **FCA discussion paper** lays out a statutory framework for overseeing the resilience of services third parties provide that many financial firms rely on. Firms are expected to have appropriate processes and controls in place to manage to disruptions, including alternative providers or contingency arrangements that can be quickly implemented.

Organisations need to treat third parties with the same diligence as their internal operation. Any risks associated with a CTP are your businesses risks and should be fully understood. Evaluating your organisation's reliance on CTP and those third parties' own levels of Operational Resilience are an integral step in understanding how able you are to prevent critical incidents and how you can mitigate the effects of such an incident.

Before entering into a contract with a third-party a comprehensive risk assessment should be undertaken to identify any potential risks such as cyber security, data protection or business continuity. Service level agreements should be comprehensive and form part of the contract as should provisions for monitoring and auditing third party performance.

Third party providers should be prepared to discuss their resilience with clients, particularly as part of contract negotiations. From our own experience, clients are increasingly asking for SLAs (Service Level Agreements) to be established within contracts to ensure operational resilience thresholds are met.

Third parties also play a key part of providing alternative solutions when disruption occurs. It is important to understand how quickly and how robust these alternatives are so they can be initiated from the appropriate part in the operational playbooks.

Have you got a **proactive approach** defined against critical incidents?

As experts in the field of Operational Resilience we often help businesses detail the important business services and the impact they have on their clients. Understand your current scenario modelling capabilities, define a proactive approach to critical incident preparedness and identify areas of improvement.

Get the right tools and structures in place to enable your CRO to own a Governance, Risk and Compliance strategy that prioritises response efforts and mitigates potential risks. Through our Clarity powered by BusinessOptix tool we can even help you build the tools and structure required to improve your operational resilience maturity.

Respond and recover from critical incidents

Having measures to **prevent and mitigate critical incidents** is an important step in your approach to Operational Resilience. But your overall strategy must address plans for dealing with a severe incident when it strikes. Large organisations and recognised brands from across the financial and commercial worlds have been exposed due to **weaknesses in their overall resilience capabilities.**

Robust response strategies can mitigate the impact of an incident on your ability to provide important business services, reassure employees, clients, and customers that you can manage a critical incident, and that you can **recover quickly and effectively with minimum disruption.**

Are your critical incident response and recovery plans ready?

To answer the question 'is your organisation critical incident ready?' it's important to consider several key factors:

- Do you understand the resources required to deliver your important business services? The criticality of the people, processes, facilities, technology and third parties should all be mapped against those services. Identifying the resources needed means:
  - You have everything **available and organised sufficiently** to be able to respond to a disruption to the organisation.
  - You can **track dependencies between key resources and identify and mitigate potential risks** associated with them.
  - You can **pinpoint resource gaps** which the organisation can then prioritise activities to mitigate.

- Your organisation's level of Operational Resilience maturity when it comes to modelling severe and plausible scenarios. How are you managing identified risks to maximise your ability to deliver your important business services? Have you developed strategies to address those risks before they become actual incidents?

- Is your organisational governance up to the task? Are business-wide processes designed and implemented with Operational Resilience in mind? It is important to ensure those processes are aware of critical dependencies, have clearly identified owners and documented procedures which are stored in a central location accessible to everyone who needs them.

  Processes should be regularly reviewed and updated to remain relevant to your business needs. Applying good governance to incident response and recovery plans will help ensure that you are continuously improving your Operational Resilience and minimising the impact of any disruptions to your operations.

- Are there workarounds for disruptions in important business services in place? Have they been tested to prove they are both realistic as well as practical and effective?

All this information will enable your business to direct investment in the right places but also be aware where you are susceptible. This may mean higher focus in these areas when considering workaround processes.

Other questions to ask to help you ensure your critical incident readiness include:

1. **Are your playbooks accessible?**

   Playbooks have a high-profile role in Operational Resilience by providing a documented, tested, and repeatable process for responding to incidents and disruptions. They offer a set of predefined procedures setting out the steps an organisation should mobilise to minimise the impact of an incident, ensure continuity of operations, and recover from the event.

   The following are some ways in which playbooks can help improve Operational Resilience by:

   - **Standardising responses**

     Playbooks help to ensure that all members of the team follow a consistent process when responding to incidents. In doing so, playbooks can reduce the risk of errors, improve the speed and efficiency of your response, and minimise the overall impact of the incident.

   - **Identifying critical functions**

     Because organising playbooks aids organisations in identify their most critical functions, processes, and systems they can then prioritise response efforts and allocate resources, accordingly, ensuring that the most critical functions are restored first.

- **Improving knowledge**

  Through testing playbooks, organisations can train their staff on the response process to ensure they are able to rapidly respond in the event of an incident.

- **Aiding continuous improvement**

  Playbooks need regular review to address changes in the organisation's environment, such as new technologies, processes, or threats. This ensures playbooks remain relevant and effective in the face of evolving risks and challenges.

Overall, playbooks are a critical component of an organisation's operational resilience strategy. They provide a structured and standardised approach to incident response, enabling organisations to minimize the impact of disruptions, ensure continuity of operations, and recover quickly and effectively from incidents.

2. Are your communications prepared?

Recently, the major high street retailer, WH Smith, was the victim of a cyber attack targeting confidential current and former employee data. Their response plan included a robust external communication strategy designed to reassure the public that customer data remained secure and stressing that trading was unaffected. Undoubtably there was also a strong internal communication response as well.

In fact, in their statement WH Smith noted:

> Upon becoming aware of the incident, we immediately launched an investigation, engaged specialist support services and implemented our incident response plans, which included notifying the relevant authorities… We are notifying all affected colleagues and have put measures in place to support them.

WH Smith's communication planning included both internal and external communications as well as notifying regulatory and law enforcement authorities. Different types of critical incidents will require different types of communication plans. However, all types of critical incidents will require employee communications – from initial response action plans through to the recovery stage – to ensure morale and engagement is not lost.

Communication plans and templates are essential tools for operational resilience because they help ensure that critical information is communicated effectively and efficiently during a crisis or disruption. Having a well-designed communication plan in place will help ensure the right people receive the right information at the right time.

Communication plans and templates are important for Operational Resilience because they contribute to and improve:

- **Consistency**

  Communication templates provide a consistent approach to communication, which helps ensure that all stakeholders receive the same message, with the same level of urgency, regardless of who is delivering the message. This consistency can be particularly important during a crisis or disruption, when miscommunications can have serious consequences.

- **Agility**

  In a crisis, time is of the essence, and delays in communication can be costly. Communication plans and templates can help ensure that messages are delivered quickly and efficiently, without the need for time-consuming deliberations or decisions.

- **Flexibility**

  Allowing for updates and modifications as the situation evolves. This can help ensure that stakeholders have the most up-to-date information, without the need for a complete overhaul of the communication strategy.

In summary, communication plans and templates are important tools for Operational Resilience because they help ensure that critical information is communicated consistently, quickly, clearly, and flexibly, even in the face of a disruptive event.

3. Do you feed lessons learned into recovery playbooks?

Lessons learned can be derived from several aspects of an organisations Operational Resilience planning. Scenario testing, where severe, but plausible potential disruptions to a firms' operation allow playbooks to be tested. Previous critical incidents, how you responded and recovered are also a great source of information for improving your Operational Resilience and should be re-examined for valuable lessons that can aid recovery in the future.

Scenario testing and exercising should be an important part of your Operational Resilience and critical incident preparedness. But unless you are taking the conclusions of testing and lessons learnt from those exercises, assessing their importance, and feeding them into improved actions and plans for mitigation and recovery, then you are wasting their potential.

While the event is fresh in the memory, these actions need to align with existing governance structures. Who are the accountable senior stakeholders? Do actions have delivery dates and clear owners assigned? How are the actions that arise from scenario testing being tracked and monitored to ensure they aren't forgotten?

Ensure that lessons are added to continuous improvement or risk action logs, that new iterations of response and recovery plans are tracked by the appropriate risk committees, and that every impacted stakeholder is apprised of new strategies and plans.

Are you ready for a critical incident?

Nobody wants the worst to happen. But, as the cases of TSB, Equifax, Royal Mail and others have shown us, critical incidents can and will occur. Businesses big and small are not immune from threats to their Operational Resilience. What we can be is **prepared**.

Being ready for a critical incident is essential for any business that wants to maintain Operational Resilience and minimise the impact of disruptions to its operations. We need to consider whether we have the necessary strategies and resources in place to survive a critical incident. This includes documenting and testing workarounds and having developed effective playbooks to utilise in the event of an incident.

By taking these steps, we can enhance our ability to respond to and recover from critical incidents, ensuring the continuity of our business operations and protecting our customers, employees, and stakeholders.

To help you determine whether your organisation is ready to face unexpected disruptions, we've compiled a list of eight essential questions that you should consider when evaluating your preparedness for critical incidents. These questions cover various aspects of Operational Resilience including resource mapping, scenario testing, Playbooks, and organisational culture.

By answering these questions, you can identify potential gaps in your business' preparedness and take proactive steps to improve your resilience:

1. Is your review cadence in place?

Regular reviews of all elements of Operational Resilience are crucial to ensure that you are prepared for a critical incident. A review of your Operational Resilience should be completed bi-annually, or annually (at the very least) to ensure that all information and workarounds are accurate and tested.

By maintaining a regular review cadence, businesses can identify and address any gaps or weaknesses in their resilience strategies, improving their ability to respond to and recover from critical incidents.

2. Do you know your Important Business Services?

Identifying and understanding the importance of those client facing business services, which if disrupted will result in material harm, will help businesses prioritise resources and focus on maintaining the continuity of critical operations in the event of a disruption. It is recommended that you document and store information regarding your Important Business Services, alongside a justification and the process for how they were identified.

3. Have intolerance thresholds been applied?

Businesses must understand the impact of losing a system or service to their clients/ customers and setting impact tolerance thresholds based on this information is an essential part of Operational Resilience planning.

Your impact tolerance thresholds should be documented, along with justification for why they were chosen, and a method for monitoring them should be established. Setting tolerance thresholds and monitoring them regularly can ensure you identify potential issues before they escalate and implement appropriate measures to minimise their impact.

4. Have you mapped your resources?

Mapping out all business resources is an essential step in developing a comprehensive Operational Resilience plan. Map your Important Business Services against various factors, including people, processes, volumes, technology, location, metrics, facilities, and critical third parties.

By mapping out their resources in this way, businesses can identify potential vulnerabilities and develop appropriate strategies to ensure continuity in the event of a disruption.

5. Can you complete scenario testing?

Businesses must have a structured and organised way to complete scenario testing against plausible scenarios, ensuring that their workaround processes achieve their aim within the required timeframe. It is important to be confident that lessons learned from scenario testing will be tracked and implemented, enabling you to continuously improve your resilience strategies.

By completing thorough scenario testing, businesses can identify potential weaknesses in their Operational Resilience plan and implement appropriate measures to ensure they can respond to and recover from critical incidents effectively.

6. Are your Playbooks and communications ready?

Playbooks should be developed, stored centrally, and signed off by appropriate business leaders. Internal and external communications should also be designed and signed off, ensuring that they are structured in a way that all levels across the business can understand.

By having these Playbooks and communication strategies in place, businesses can minimise the impact of disruptions to their operations and ensure continuity, while also protecting their customers, employees, and stakeholders.

7. Is your governance structure fit for purpose?

A robust governance structure is critical for effective Operational Resilience. This includes top-to-bottom accountability with governance committees at the right level, looking at the relevant risks and mitigations to make key business decisions and absorbing the lessons learnt from scenario testing and previous incident responses.

It is also essential to have a system for tracking and reporting lessons learned, ensuring continuous improvement. A fit-for-purpose governance structure ensures that all stakeholders are aware of their roles and responsibilities, and that all risks are adequately addressed.

8. Is your culture resilient?

It is essential that everyone in the business understands their role in managing risk and that risk management is embedded across the entire employee lifecycle. Promoting a resilient culture at all levels and featuring Operational Resilience across the culture empowers your employees. Helping them to identify and manage risks effectively, leading to better decision-making and increased overall resilience.

If your answer to any of the above questions is no, **it's time to act!**

Failing to address gaps in your Operational Resilience capabilities could put your business at risk. Leading to significant disruptions to your operations, substantial financial losses, as well as damage to your reputation.

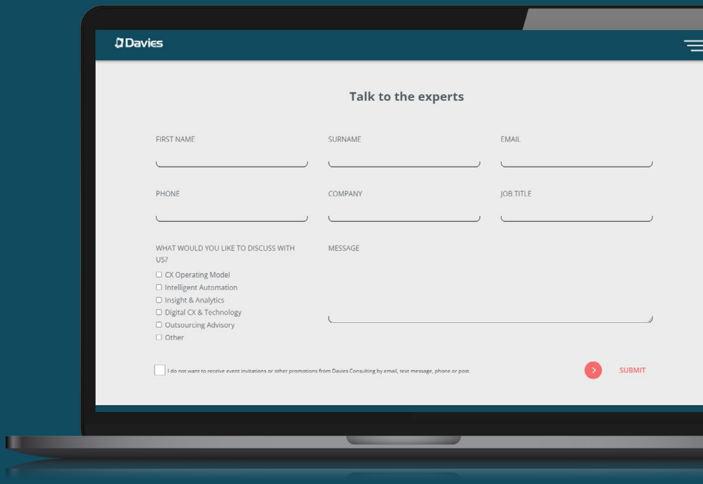
To ensure that your business is fully prepared for critical incidents, you may want to consider working with a trusted consulting firm, such as Davies, who can provide expert guidance and support in developing and implementing an effective Operational Resilience strategy.

How Davies can help

Davies has **pioneered a robust methodology** which has helped businesses improve their Operational Resilience and provided them with the tools required to **manage their Operational Resilience going forward.**

Over 7 weeks we work closely with key stakeholders to **assess your enterprise-wide Operational Resilience.** In doing so we map your maturity, identify vulnerabilities, provide baseline tolerances, and support you with actionable recommendations that reduce and mitigate risk.

If you would like to learn more about how Davies holistic approach can help you **enhance your Operational Resilience and protect your business, contact us now.**



Talk to the experts

FIRST NAME

SURNAME

EMAIL

PHONE

COMPANY

JOB TITLE

WHAT WOULD YOU LIKE TO DISCUSS WITH US?

- □ CX Operating Model
- □ Intelligent Automation
- □ Insight & Analytics
- □ Digital CX & Technology
- □ Outsourcing Advisory
- □ Other

MESSAGE

□ I do not want to receive event invitations or other promotions from Davies Consulting by email, text message, phone or post.

SUBMIT

Get in touch

David Ilett
Consulting Director,
Davies Consulting

David.Ilett@davies-group.com

Michael Anderson
Vice President - Client Management,
Davies Consulting

Michael.Anderson@davies-group.com

Mark Odlin
Senior Consultant,
Davies Consulting

Mark.Odlin@davies-group.com

Jason Pillay
Senior Consultant,
Davies Consulting

Jason.Pillay@davies-group.com

Davies

Davies Group

DISCLAIMER: This document is intended for general informational purposes only, does not take into account the reader's specific circumstances and is not a substitute for professional advice. Readers are responsible for obtaining such advice from licensed professionals. The information included in this document has been obtained from sources we believe to be reliable and accurate at the time of issue. The issuer disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and any acts or omissions made based on such information.

Davies Group Limited (Company Number 6479822). Registered office: 5th Floor, 20 Gracechurch Street, London, EC3V 0BG

davies-group.com

@Davies_Group

Davies Group

CON-JL-0423-4197437705