Operational Resilience
Mitratech's Alyne
White Paper

MITRATECH

Driving a Modern Operational Resilience Program

Time to strengthen your operational resilience processes, meet the latest regulatory requirements in this space, ensure operational success and deliver far greater proficiency with the help of high-performance technology.

Introduction

Operational resilience refers to the processes put in place within an organization that aim to increase Business Continuity Management (BCM) programs in order to focus on the risk impact, risk appetite and tolerance levels for disruption within the organization's internal and external ecosystem (third-parties).

Operational resilience processes encompass crucial risk management capabilities like: risk assessments, risk monitoring and continuous controls that impact workforce, processes, facilities, IT infrastructure and third-parties.

The Bank of England, defines Operational Resilience as:

"The ability of firms, and the financial sector as a whole, to absorb and adapt to shocks, rather than contribute to them."

The Financial Conduct Authority (FCA) echoes this sentiment by stating that a financial system that is resilient owns the ability to:

"Absorb shocks rather than compound them."

The financial regulatory bodies collective approach towards operational resilience has not undergone many changes since the publication of the combined 2018 paper by the FCA and the Prudential Regulation Authority (PRA), regulated by the Bank of England.

As part of the drive to make the UK's financial sector more resilient, regulators have been implementing measures to financially penalize organizations if they incur in extended failures in their business services due to inaction, despite being given sufficient time to prepare.

As a result, most firms have recognized the need to take action and have already started to plan and implement projects to cover the necessary review of their services.

The Systematic Lens of Operational Resilience as a Regulatory Imperative

While operational resilience as a term is fairly new, the concept of managing operational risk and increasing resilience within organizations is not.

After the 2008 financial crisis, the development of new rules and frameworks for financial reporting and resilience came into focus. Since the beginning of the COVID-19 pandemic, the topic of operational resilience rose to the top of the regulatory agenda with an even sharper focus.

As a direct result, regulators have been releasing publications campaigning for greater operational resilience, highlighting the potential areas of disruption to firms, and subsequently their customers, across a variety of business operations.

Technology-led business transformation, high-profile instances of disruption, and recognition of the interconnectedness of the financial sector have all led to increased attention on operations.

Recent Regulatory Updates Touching Operational Resilience

1. UK SOX

UK SOX is the unofficial name given to the new corporate governance regulation of the UK. The British government has announced details of its corporate governance reforms which will move the UK's regime closer to the US Sarbanes-Oxley regulation.

This new regulation places substantial new reporting requirements on directors and will require public disclosures from these on:

- **Responsibility Statement**
- **Statement on Fraud**
- **Resilience Statement**
- **Audit and Assurance Policy (AAP)**

2. DORA

In December 2022, the EU introduced the financial services act, Digital Operational Resilience Act (DORA), which forms part of the European Commission's wider Digital Finance Strategy.

The regulation addresses the digital resilience needs of regulated financial institutions, establishing oversight on critical Information and Communication Technology (ICT) service providers.

This regulation aims to ensure mature third-party risk management programs, within the financial services industry, and improve cyber resilience.

3. CP19/32

The Bank of England and the Prudential Regulation Authority (PRA) have developed, in partnership, proposals to CP19/32 in order to improve the operational resilience of the UK financial services sector.

4. CPS230

In July 2022, the Australian Prudential Regulator (APRA) began consultations on the new Prudential Standard, CPS 230 Operational Risk Management (CPS 230).

The aim of this Prudential Standard is to ensure that an APRA-regulated entity is resilient to operational risks and disruptions. Meaning, an APRA-regulated entity must effectively manage operational risks, maintain core business operations through disruptions, and contemplate third-party risk management.

Clearly, operational resilience is an increasingly important and urgent priority for financial services regulators across the globe and is rapidly rising-up the strategic agenda of financial services firms' Boards and senior management teams.

While regulatory bodies are often focussed on common goals, they usually have different perspectives and approaches. This is the same for the regulatory requirements revolving around operational resilience.

Why is Operational Resilience Important?

Regulatory requirements have been pushing business leaders to consider operational resilience as an integral element in their business strategy because it offers decision-makers a clear understanding of their end-to-end processes, shining the spotlight on critical infrastructures and dependencies.

Factors such as technological advancement, the ever-changing cyber risk landscape and events such as COVID-19, have propelled executives to prioritize operational resilience and drive change in necessary and vulnerable areas.

Operational resilience should be at the top of the agenda of all organizations, no matter where in the world they are geographically located. However, there are benefits to implementing the UK's approach to operational resilience as it is largely similar to regulations that are required in other geographical locations.

When understanding that operational resilience encompasses third-party risk management, the importance of this focus area couldn't be more obvious. Organizations in all industries have been increasingly outsourcing business processes to third-parties across their value chain, creating new entry points for potential business disruptions.

Considering the cost of disruptions, both direct and indirect, it is only financially and logically reasonable to put operational resilience at the top of your business goals in view of the certainty it offers to daily business operations.

Managing operational resilience in organizations is an amalgamation of three key GRC use cases firms should already be addressing, namely:

1. Business Continuity Management (BCM)

The primary focus of operational resilience is to ensure that even under the emergence of new threats and vulnerabilities, firms have planned for contingencies with a comprehensive and successful BCM plan.

In times of disruption and crisis, BCM helps to ensure operational resilience by maintaining core business operations while minimizing cost, damage and recovery time.

While it is fundamentally impossible to avoid all operational risks, having the ability to ensure business operations during adversity, creates a powerful competitive advantage within your organization's value proposition.

2. Operational Risk Management

As business processes, infrastructures and external factors become increasingly more interconnected and complex, having the capabilities necessary to effectively manage operational risk, creates a comprehensive framework for assessing risk across the business.

The COVID-19 pandemic certainly exacerbated operational risks that hadn't been contemplated in such a scale before and increased uncertainty of business outlook. As a result, the importance of having an operational risk management program in place and effectively addressing any risks that threaten the stability of critical operations, is imperative.

Why is Operational Resilience Important? (Cont.)

Having a comprehensive operational risk management program that focuses on critical operations and their interdependencies, in preparation for a range of plausible scenarios, will contribute to mature Enterprise Risk Management (ERM) capabilities within your organization.

In essence, organizations should have sufficient controls and procedures in place in order to identify internal and external threats and vulnerabilities. In order to conceptualize a well thought through operational resilience framework, the operational risk function should strive to work closely with the BCM function to minimize exposure to disruptive events. Simply put, a well-integrated plan is necessary to achieve operational excellence.

3. Third-Party Risk Management (TPRM)

Financial services organizations often engage with multiple third-party vendors and intragroup entities to deliver critical operations. With greater reliance on third-party services to scale and deliver business operations, it is imperative that financial services institutions manage their supplier dependencies by developing appropriate TPRM procedures and exit strategies in the event of a third-party failure or business disruption.

Remaining consistent with critical business operations across third-party dependencies is a key risk to address, as even a single point of failure of a service provider can potentially snowball into greater disruption in operations.

From a regulatory perspective, there has been a strong focus on vendor governance and third-party resilience. In fact, many regulatory authorities, such as the PRA, require firms to notify before a material outsourcing decision has been finalized with a detailed follow-up proposal.

As part of an effective vendor governance framework, the scope of many industry standards such as: ISO 27001, NIST C2M2 and COBIT 5, form a critical component of an organization's risk management program and overall operational resilience.

What does this mean in a business context?

Risks to an organization can span across many areas, but primarily, we should consider those that translate into an interruption to one or more of the following:

- **Office / Working Premise:** An example of this could be an outage of power to the premises or any number of factors that might lead a working space to close its doors to employees. After the pandemic, hybrid working has become a new normal across the globe. Office spaces are becoming less necessary, which brings a new set of opportunities and challenges to be considered.
- **People:** This could be anything that threatens the human element of the organization. From a low staff retention rate, slow quitting, or lack of qualified personnel to external factors like a virus pandemic for example.
- **Information Technology:** A failure in an organization's IT infrastructure or a cyber attack, for example.

Why is Operational Resilience Important? (Cont.)

- **End-to-End Business Operations:** This could be anything that affects the end-to-end services and/or business operations of our organization. Meaning, all outsourced processes to third-parties should be carefully analyzed.
- **ESG:** Environmental, Social and Governance (ESG) factors are part of our day-to-day. Failing to contemplate these into a risk framework could be severe, both from a regulatory and a reputational point of view.

Even if you contemplate risks that span all of these different areas and beyond, the goal in a mature risk framework is to fully cover and harmonize all of the areas listed above under one unified approach.

This creates a coherent structure that presents your organization with an evidential view of the totality of these focus areas. More importantly, it increases the knowledge of decision-makers and formalizes their understanding of potential gaps that need to be addressed.

Timeline of Requirements for the UK Operational Resilience Regulation

While most financial services institutions have already implemented operational resilience programs in line with the consultation papers set out by the Bank of England, the Financial Conduct Authority (FCA), and the Prudential Regulation Authority (PRA); two new regulatory deadlines have been introduced in the final policy statement on operational resilience.

1. Implementation Period

Impacted organizations were given one year to identify critical business services and operationalize their policy framework.

2. Transitional Period

UK regulators expected impacted organizations to have completed all preparations in place as well as an initial self-assessment. This date marks the end of the implementation period and the beginning of the three year transitional period.

3. Deadline

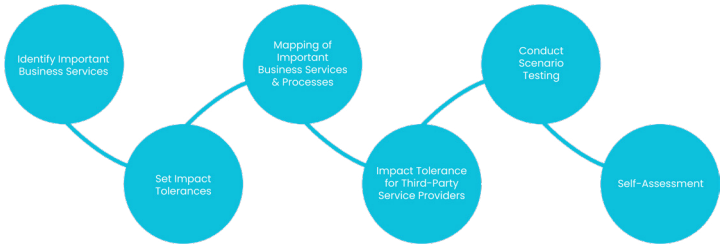
This date marks the end of the transitional period. Meaning all firms must have performed all mapping and testing, demonstrating that they have made all necessary efforts to remain within their defined impact tolerances.

An Integrated Approach to Operational Resilience

Operational resilience is a broad regulatory topic rather than a highly defined regulation, which makes it inherently challenging to establish in view of the ever-changing and evolving threat landscape. Regulators will be placing a large focus on the strategy and approach that firms take, as well as how seriously the topic is taken by Boards' and senior management.

In formulating their operational resilience framework, decision-makers will exercise their governance structure to define important services, identify tolerances, map processes, test and implement the best approach to ensure continuous delivery of business operation.

In addition, they also have to ensure that resources are strategically and appropriately allocated to support their operational resilience program. In order to align with the UK operational resilience requirements, firms will need to perform and maintain a number of crucial steps before the deadline of March 2025.



1. Identify Important Business Services

Firstly, organizations will be required to identify important business services they provide to customers. Important business services are those that, if impacted, would most likely cause severe disruptions to customers.

This analysis will be unique to most organizations, as each business has critical differences, varying from geographic location, to specific product offerings.

In identifying these services, financial institutions must consider the following factors:

- **Who would be affected by the disruption of the service?**
- **What is the impact of disruption on the firm itself?**
- **What is the overall economic impact it might have on the broader UK financial system?**

As customers are the ones directly affected by the disruption, firms must adopt a 'business services first' view and identify what services are integral for customers and their experience as a whole.

2. Run Business Impact Assessments (BIA)

After understanding the business domains, and in order to anticipate how best to respond to a disruption, business leaders need to conduct an evaluation to further understand their customers core requirements and identify the most important services.

In doing so, organizations can make resilience considerations in the design of the most vulnerable organizational assets to plan the best course of action in the event of a crisis. Likewise, business firms will also need to identify operational dependencies such as staff, data, suppliers and locations which directly support the customer experience and where disruption could have the greatest impact. This will support a comprehensive view of the dependencies of critical business services.

An Integrated Approach to Operational Resilience (Cont.)

where disruption could have the greatest impact. This will support a comprehensive view of the dependencies of critical business services.

Running a Business Impact Assessment (BIA) will strengthen the firm's oversight as it adopts a consistent approach to obtaining deep understanding of each key service, helping to define a clear operational resilience strategy based on the different criticalities of business services identified.

Holding a consolidated, centralized, view of each key service will provide a solid foundation for organizations to incorporate future services and improve management's overall business understanding, with the purpose of making well-informed investment decisions.

3. Set Impact Tolerances

As mentioned before, there are different approaches to operational resilience based on geographical factors. In the US or the EU for example, there is no concept of impact tolerances. However, impact tolerance forms the foundation of the UK's regulatory requirements.

According to the UK proposal, impact tolerances are defined as the firm's measure for disruption to a particular business service. Notably, the UK regulators have emphasized that impact tolerance is not the same as risk appetite metrics.

To begin, firms should assume the maximum level of disruption to their systems and processes supporting the services. In response to these disruptions, firms should set an impact tolerance in consideration of their ability to resume delivery of important business services. These tolerances should be set at a point where disruption to an important business service would cause severe levels of operational harm to the end customer.

These impact tolerances are intended to steer the Board's and senior management's decision to prioritize operational resilience, as it emphasizes that disruptions to a business service are inevitable and must be actively managed. Hence, these impact tolerance should be communicated clearly to guide Board decisions on investment, risk management, business continuity management and corporate structure.

4. Mapping of Important Business Services & Processes

To obtain a bird-eye view of the resources that your organization deploys to deliver important business services, your firm should conduct a 'mapping of resources' to identify and clearly document all resources used within the organization, these include: technology, data, people, facilities, third-parties and key processes.

The act of mapping an important business service guides and assists your firm to identify vulnerabilities and/or weaknesses in the delivery of important business services. With the mapping in place, your business can test its ability to respond and recover within its impact tolerances.

An Integrated Approach to Operational Resilience (Cont.)

5. Impact Tolerance for Third-Party Service Providers

To deliver important business services, firms often engage with third-parties in an effort to outsource processes with the aim of making operations easier. Extensive coordination is necessary to ensure that provisions for third-parties also meet the thresholds set out for the firm's impact tolerances.

All stakeholders involved in a specific process, the firm itself and the responsible service provider, need to work together to address risks to operational resilience, which arise from the interconnectedness of the environment in which the firm operates. This demands a critical degree of transparency and trust.

Vendor governance and/or Third-Party Risk Management (TPRM) practices should be used to extensively evaluate each third-party – from the service they provide to the third-parties they themselves use.

For example, a third-party service provider of yours could also be engaging with another business for cloud services. In the event the third-party becomes insolvent, a formal takeover agreement should be put in place to ensure a continuation of the overall service. This is just one example that highlights the importance of assessing and analyzing end-to-end provisions to ensure the ongoing viability of your firm, under any circumstances.

For a firm to be operationally resilient they must be able to effectively manage their third-parties. They need to consider their dependencies and the level of resilience these third-parties actually have.

According to the FCA, issues with third-parties such as IT failures to an important supplier account for 15% of operational incidents. This demonstrates how increasingly reliant firms and their end customers are on their third-parties and why they need to be managed to minimize risks.

To ensure effective oversight, firms should run assessments against all third-parties critical to the business infrastructure. By gaining evidence through assessments the organization will be able to identify any potential weaknesses that might pose a threat to the firm and increase the risk of disruption of important services.

6. Conduct Scenario Testing

Having set impact tolerances for different business services, it is imperative for firms to test their ability to remain within these tolerances in the event of a severe, but plausible, disruption to their operations.

Conducting scenario testing allows business leaders to verify the resilience levels of their services and identify areas that require more operational resilience measures.

When conducting scenario testing, it is important to bear in mind that impact tolerances are defined with the assumption that disruptions have already taken place. Hence, the focus of scenario testing should be on the response and recovery actions rather than estimating the probability of the incident taking place. Simply put, it should be proactive rather than preventive in nature.

An Integrated Approach to Operational Resilience (Cont.)

When carrying out a scenario testing, these are a few steps your firm should follow:

- **Specify an Appropriate Range of Adverse Circumstances**

  Firms should specify an appropriate range of adverse circumstances, varying in nature, severity and duration, based on the specific business and risk profile.

- **Test on a Range of Scenarios**

  Test on a range of scenarios in which supporting resources for one or more of their important business services have been disrupted.

- **Identify Gaps in Current Resilience Measures**

  Understanding situations where it isn't possible to stay within your impact tolerance will be crucial, and will enable firms to identify gaps in their current resilience measures in order to assess what actions they need to take to improve.

  Previous incidents or 'near misses' that the firm may have experienced before can be used as a reference point to inform which scenarios to test.

- **Review and Improve**

  To align with the new requirements coming into force, firms should revisit and review existing business continuity and disaster recovery plans. Extensive and thorough testing will provide assurances that each service is effective and resilient to the specific scenarios designed for the exercise. These scenario tests may also highlight undiscovered weaknesses that have arisen since the previous testing was conducted and will require further improvements or changes to systems, processes or people.

7. Self-Assessment

To ensure that there is a sound operational resilience framework in place, it is critical to establish clear lines of responsibility and accountability. This can be achieved through clear guidelines and current expectations in a self-assessment.

Self-assessments should include details of your organization's operational resilience framework, such as:

- **Important business services and their impact tolerances.**
- **Principle of your business approach mapping.**
- **Description of your scenario testing strategy.**
- **Description of vulnerability remediation.**

While firms are not legally required to submit their self-assessments periodically, they will be required to produce these documents upon request.

As a result, and according to the Bank of England, this document should be regularly reviewed by the Board and senior management to ensure the document remains fully comprehensive and proportionate to the nature, scale and complexity of the firm's services. In other words, it should be reflecting the organization's current risk profile at that point in time.

Board and Senior Management Oversight

To set effective standards for operational resilience practices, the Board and/or senior management should be actively engaged in the process of managing business risks relevant to this discipline. Board members should be equipped with adequate knowledge, skills and expertise to identify the important business services to the firm, understand the mapping process, set impact tolerances and evaluate the firm's ability to remain within these impact tolerances.

In reality, this is an initiative that can be delegated down to risk and compliance functions to develop across the firm. However, the proof and evidence required to demonstrate the firm's approach need to be actively engaged with the board early on.

Under the UK's Senior Manager & Certification Regime (SMCR), Board members need to sign off on the self-assessment confirming their firm's resilience, and can be held personally liable should they not be able to demonstrate that their decision-making to the chosen approach was sound.

Approaching operational resilience as an annual "tick-the-box" exercise will no longer be acceptable in meeting requirements, nor will it be helpful in providing firms with the response and recovery speed that a business disruption or outage might require. Continual assessment is needed, with oversight from the Board, to validate the issues and vulnerabilities identified in order to ensure appropriate investment decisions are made.

Executive sponsorship and ownership should be run by the entire Board, especially those mandated by senior management functions and not viewed purely as an IT initiative to be fulfilled by the COO/CFO.

How Mitratech's Alyne Can Help

The COVID-19 pandemic contributed to greater technological adoption and increased the regulatory pace towards a more robust operational resilience framework for financial institutions.

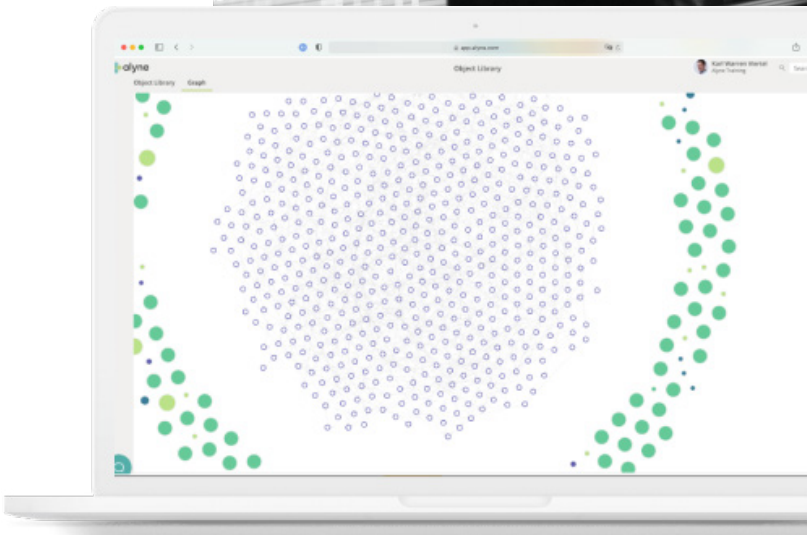
As regulators sharpen their focus on this topic, Mitratech's Alyne GRC solution helps businesses meet their requirements by digitizing and automating processes.

1. Define Important Business Services as Objects

Identify and capture information of all Important Business Services (IBSs) within your organization. Using Alyne, you are able to customize the default information attributes within our application through a simple point and click interface.

Using Alyne's Object Library, you can gain a full mapping of the relevant business services. This will then provide you with a deep understanding of the full implications of different scenarios that could cause a disruption to the business.

Alyne provides comprehensive support to bring together the many layers and interconnected ecosystems of the identified key services, sub-services, IT landscape and links to third-parties. By providing a navigable and dynamic visual representation of how services are connected, Mitratech's Alyne is able to deliver an immediate holistic overview of the organization's internal and external business landscape.



:

How Mitratech's Alyne Can Help (Cont.)

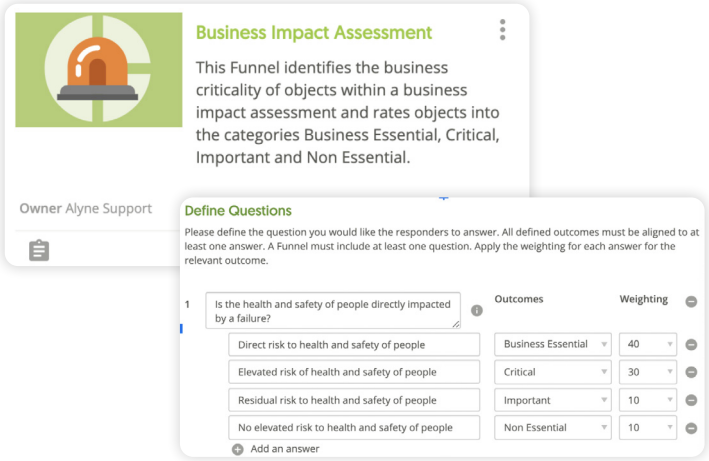
2. Perform Business Impact Assessment Funnels for Each Service

Alyne's intuitive and easily customisable zero-code workflow funnels offer a consistent, coordinated and measurable approach to help you classify and identify which services and sub-services are core to your business operations.

This allows you to have a complete end-to-end view of people, processes and technology so that you can triage your assets, launch smart workflows and make informed decisions.

Mitratech's Alyne solution includes a number of ready-to-run funnel templates, including:

- **Business Impact Assessments**
- **Outsourcing Classification**
- **Material Business Process Outsourcing**
- **Vendor Risk Classification and more**



3. Define an Operational Resilience Control Set to Perform Self-Assessments Across the Business

- **Measuring Maturity of Controls According to CMMI**

  Depending on the industry and company size, different organizations may adopt different maturity models based on their stages of compliance.

  By providing a common benchmark, Alyne classifies and gives examples for organizational attributes and processes based on the Capability Maturity Model Integration (CMMI) levels, to provide clear guidance enabling organizations to easily classify and identify their maturity level. This will serve as a guide on how business leaders can improve their processes based on the 5 levels outlined by CMMI.

- **Digital Assessments to Measure Maturity at Scale**

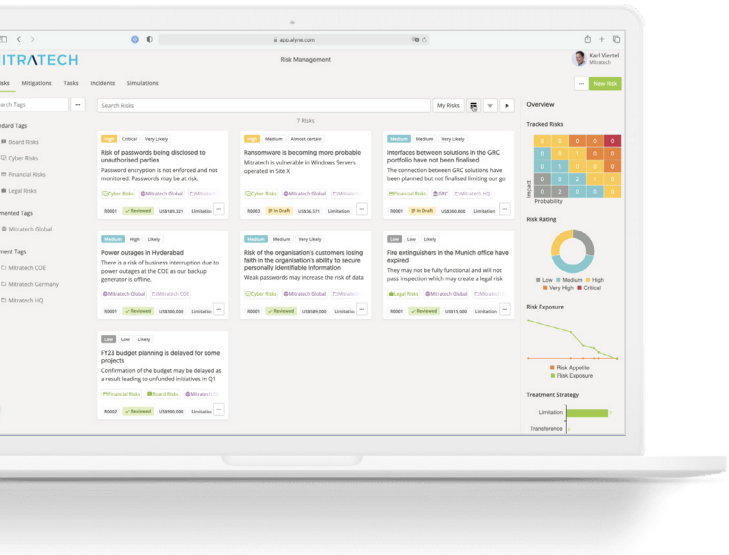
  For example, using the FCA and PRA Cyber Security and Risk Management Control Set available within Alyne and running baseline assessments against your cyber security requirements allows you to easily obtain a maturity overview of your existing controls based on a defined benchmark, provided by Mitratech's Alyne solution. Assessments in Alyne are highly configurable, and have the ability to be sent at scale across your organization and third-parties.

How Mitratech's Alyne Can Help (Cont.)

4. Risk Management

Alyne's risk register helps organize risks across trivial, generic and complex dimensions according to the organization's specific business needs. It supports and simplifies tedious and oftentimes, error-prone, risk management processes by allowing users to cluster risks easily, based on a different combination of risk dimensions. This provided a holistic overview of risk combinations.

Furthermore, within Alyne's risk register, you are able to set impact tolerances for each risk tag and implement mitigation measures and controls for each risk identified, in order to reduce overall risk exposure. To facilitate collaboration across your enterprise, you can also assign tasks to mitigation owners within the platform.

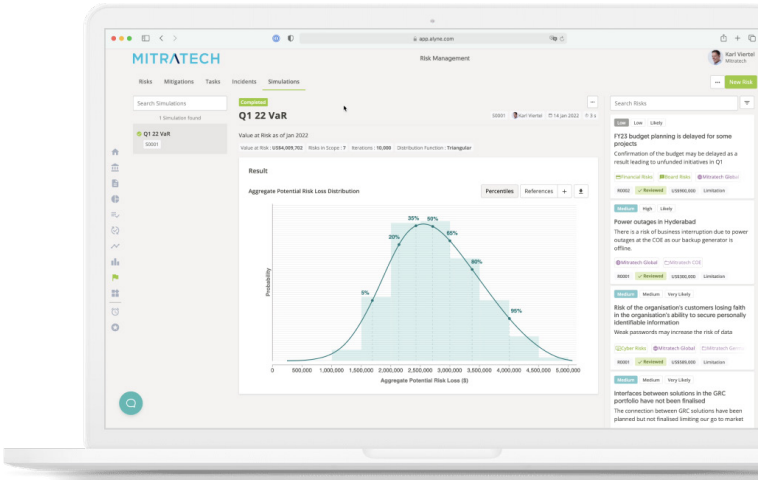


- **Monte Carlo Simulations**

Coupled with Alyne's built-in financial loss estimator to quantify your potential risk loss, Alyne's platform incorporates next-generation functionality to help business leaders conduct quantitative risk analysis by using Monte Carlo simulations to calculate true Value-at-Risk (VaR).

The process of performing a Monte Carlo simulation can often take days, if not weeks. However, Alyne's platform leverages scalable serverless infrastructure which allows you to perform the simulation in a matter of seconds, across different organizational segments, on tens of thousands of risks.

Alyne's built-in Monte Carlo simulations can help business leaders place a financial figure on resilience by quantifying the operational risks that the organization is being exposed to. This allows for a better communication of the true risk exposure of the business, in a way that the Board and/or investors can understand, and proper justification of the importance of their resiliency program.



In Closing

Organizations must focus on the core business services they offer and map out the end-to-end journey of how they are delivered combining technology, people and processes.

Furthermore, they must agree internally on the impact tolerances that are acceptable for the end customer, invest in building operational resilience practices into those identified focus areas through scenario testing and aim to remain within the agreed tolerances.

UK regulated financial services institutions can only expect to be required to meet a higher bar and standard in the future as the regulatory bodies become increasingly involved. To ensure that processes operate seamlessly and smoothly across different functions within the firm, reporting lines and across geographies; businesses should take ownership to drive operational resilience with the right focus. Meaning, ensuring that an impact tolerance is not breached and be prepared for any disruptions that may come their way in order to move from a place of uncertainty to stability.

About Mitratech

Mitratech is a proven global technology partner for corporate legal, GRC, and HR teams seeking to maximize productivity, decrease costs, and mitigate risks by deepening operational alignment, increasing visibility, and spurring collaboration across their organizations. By partnering with customers to design, develop, deliver and support the best legal, GRC, and HR software solutions on the market; Mitratech enables departments to become hubs of efficiency, innovation and excellence for the entire organization.

Mitratech's Platform provides expert product offerings to organizations worldwide, supplying end-to-end solutions that enable them to implement best practices and standardize processes across all lines of business, as well as effectively manage risks and ensure business continuity.

Mitratech serves over 7,000 organizations worldwide, spanning more than 160 countries.

For more information, please visit: www.mitratech.com

MITRATECH

info@mitratech.com
www.mitratech.com