metricstream

EBOOK

REVISITING THE CHALLENGE TO DELIVERING A STATUS OF **OPERATIONAL RESILIENCE IN FINANCIAL MARKETS** THROUGH AN INTEGRATED RISK MANAGEMENT APPROACH

By Charles Nicholls,
Senior Sales Executive at MetricStream

Table of Contents

Foreword

Much before the COVID-19 pandemic, regulators were already focusing substantially on regulations and reporting standards to ensure compliance by the board and senior management, delivering a determined level of operational resilience.

In the UK, the Bank of England (BoE), the Financial Conduct Authority (FCA), and the Prudential Regulation Authority (PRA) published a joint discussion paper on Operational Resilience in 2018 followed by a joint consultation paper in 2019 with the primary objective of promoting the operational resilience of firms and financial market infrastructures (FMIs).

Similar efforts were made by regulators in other jurisdictions. In the European Union, draft legislation, Digital Operational Resilience Act (DORA), was published in 2020. In the U.S., federal bank regulatory agencies released a paper in October 2020 outlining sound practices for large banks to help them enhance operational resilience.

Given the continued market focus on this subject, this eBook aims to present prevailing views from across industry professionals and consultants. It explores what operational resilience really means in practice and how organizations can gain a view and report to the board, investors, and regulators in an agile and meaningful fashion to attest to their “State of Operational Resilience”.

Definitions and Regulators

What is Operational Resilience?

Isn't it just an extended business continuity management plan to extend beyond data processes? Should the responsibility sit within risk and compliance or just the IT and operational systems processing teams?

To get an understanding of the definition, we need to look at the context and as we are looking at financial markets, the definition is subject to the related regulator's definition. In the joint Consultation Paper, the Bank of England defined operational resilience as:

"the ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions".

This does not change in the policy statement but is further detailed in the associated Operational resilience: Impact tolerances for important business services:

The policy requires firms and FMIs to set, and take actions to meet, standards of operational resilience that incorporate ***the public interest*** *as represented by* ***supervisory authorities' objectives.*** *Firms and FMIs should focus on their* ***important business services*** *and ensure they have the ability to* ***remain within impact tolerances in severe but plausible (or extreme) scenarios****. Firms will be required to* ***map the resources, people, processes, technology and facilities necessary to deliver important business services****, irrespective of whether or not they use third parties in the delivery of these services, and* ***test their ability to remain within their impact tolerances.***

In Europe, the draft Digital Operational Resilience Act (DORA) was published in September 2020 arising from the European Systemic Risk Board (ESRB) in February 2020 where their report concluded that:

"A cyber incident can evolve into a systemic crisis when trust in the financial system is eroded…The ESRB has therefore identified cyber risk as a source of systemic risk to the financial system, which may have the potential for serious negative consequences for the real economy."

The Basel Committee on Banking Supervision's (BCBS) "Principles for Operational Resilience", published in August 2020, together with the "Revisions to the principles for the sound management of operational risk", states:

"While significantly higher levels of capital and liquidity have improved banks' ability to absorb financial shocks, the Committee believes that further work is necessary to strengthen banks' ability to absorb operational risk-related events, such as pandemics, cyber incidents, technology failures or natural disasters, which could cause significant operational failures or wide-scale disruptions in financial markets. In light of the critical role that banks play in the operation of the global financial infrastructure, increasing their resilience would provide additional safeguards to the financial system".

"Operational resilience is an outcome that benefits from the effective management of operational risk.

Activities such as risk identification and assessment, risk mitigation (including the implementation of controls) and ongoing monitoring work together to minimise operational disruptions and their effects.

An operationally resilient bank is less prone to incur untimely lapses in its operations and losses from disruptions, thus lessening their impact on critical operations and their related services, functions and systems. While it may not be possible to avoid certain operational risks, such as a pandemic, it is possible to improve the resilience of a bank's operations to such events…"

“The Committee defines operational resilience as the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption. In considering its operational resilience, a bank should take into account its overall risk appetite, risk capacity and risk profile.”

Materiality is key again here and the implied focus that the response expected by the regulator is commensurate with the risk capacity the organization can withstand. How can organizations assess this if they don’t incorporate it into their core operational risk framework? Organizations need a powerful integrated risk management platform for a 360-degree view of their risk profile.

The European Central Bank’s (ECB) positioning statement regarding supervisory cooperation on operational resilience states:

“Operational resilience has always been important to the safety and soundness of financial firms and the stability of the financial system. The ability of a bank to recover from an operational disruption— such as a cybersecurity incident or a natural disaster—has become even more important with the growing trend toward technology-led business transformation”.

…

“The ECB recognizes the global and interconnected nature of banks and the importance of supervisory coordination and is committed to working closely with the Federal Reserve and the UK Prudential Regulatory Authority to ensure that supervisory approaches on operational resilience are well coordinated”.

And, ESRB’s guidance on “Operational Continuity in Resolution” gives more detailed specific requirements and a targeted timeline:

“As outlined in the Expectations for Banks (EfB), operational continuity in resolution (OCIR) refers to the ability to effectively implement, from an operational point of view, the resolution strategy and, consequently, to stabilise and restructure the bank.

To achieve this, banks are expected to:

a) identify all relevant (i.e. critical and essential) services, as well as underlying relevant operational assets and staff/roles, and map them to the legal entities, providers and recipients, core business lines (CBLs) and critical functions (CFs) (mapping interconnectedness for operational continuity);

b) ensure that relevant contractual arrangements with both third-party and intra-group legal entity providers are clearly and comprehensively documented, kept up to date, and are mapped to relevant services;

c) assess the operational continuity risks in resolution, such as the interruption of relevant services, loss of access to relevant operational assets and unavailability/vacancy of relevant staff/ roles;

d) mitigate the identified operational continuity risks by putting in place appropriate operational arrangements (e.g. resolution-resilient service contracts);

e) have in place cost and pricing structures for services which are predictable, transparent and set on an arm’s length basis;

f) ensure the financial resilience of service providers;

g) have in place management information system (MIS) capabilities that provide timely access to the up-to-date information needed to identify potential operational continuity risks to resolution, and to carry out separability and restructuring (e.g. repository of the contracts governing provision of the relevant services);

h) ensure adequate governance arrangements for OCIR purposes (resolution planning and execution)

These stated expectations and guidelines and those contained within the European Banking Authority's (EBA) Guidelines for outsourcing Section 4; 31 (b):

"31. When assessing whether an outsourcing arrangement relates to a function that is critical or important, institutions and payment institutions should take into account, together with the outcome of the risk assessment outlined in Section 12.2, at least the following factors:

- a) *whether the outsourcing arrangement is directly connected to the provision of banking activities or payment services for which they are authorised;*
- b) *the potential impact of any disruption to the outsourced function or failure of the service provider to provide the service at the agreed service levels on a continuous basis on their:*
  - i *short- and long-term financial resilience and viability, including, if applicable, its assets, capital, costs, funding, liquidity, profits and losses;*
  - ii *business continuity and operational resilience;*
  - iii *operational risk, including conduct, information and communication technology (ICT) and legal risks;*
  - iv *reputational risks;*
  - v *where applicable, recovery and resolution planning, resolvability and operational continuity in an early intervention, recovery or resolution situation;"*

All these factors closely align and highlight the expansion beyond simple business continuity management and third-party management.

In the US, the Federal Financial Institutions Examination Council (FFIEC) and the Federal Reserve seem to be following much of the same reviews with an increased focus on large financial institutions (LFI's).

In the Asia Pacific region, the Monetary Authority of Singapore (MAS) regulations also focus currently on cybersecurity, technology risk, and the reliance on third parties and obligations through outsourcing as do the Australian Prudential Regulatory Authority (APRA) standards and all seem to align with the same core focus.

The duty of care implied by the UK regulators' consultation paper extends beyond just the traditional investor/shareholder emphasis but declares a further altruistic focus on the global market in which the entity operated and even the world with increasing expectations to include Environmental, Social and Governance (ESG) considerations. Diversity and inclusion are also playing a considerable added factor to manage and prepare for the new normal.

In conclusion, the scope and definition are still being formed and expanded upon by the various regulators but seem strongly aligned.

What are the Goals and Why the Regulatory Focus?

Regulators only tend to act in response to failures.

Pre-pandemic, the spate of public company failures of both internal audit and external audit and sufficient board and senior management insight had many repercussions. Most notably in the role of management and culpability, the UK Prudential Regulation Authority's (PRA) Senior Managers Regime was updated and significantly extended under the Senior Managers Certification Regime (SMCR). Many key business failures in the UK in construction and retail such as Carillion and BHS in the UK also gave rise to the UK Government commissioned Brydon Report into the Quality and Effectiveness of Audit.

One of the concluding recommendations from that report is to move the traditional focus to reflect on the business as a "Going Concern "and a "True and Fair" view of the audit report to be replaced with the term "present fairly, in all material respects".

Section 24 on Technology of this report also applies to the topic of delivering a view to the state of operational resilience. Here, we see the independent review determining the need for a move to continuous assessment and assurance through technology and the traditional reliance on annual reviews having significantly reduced relevance due to the ever-changing global market environment and delays associated with being able to take actionable responses to breaches, errors, fraud or crime incidents, and near-miss events.

Closer to home in the banking world, it was IT systems failures that were crippling the market having a huge impact on retail banking, but they were not alone. Ransomware attacks, DDOS attacks, and geopolitical hacking threats have become prominent across many global banking and financial services institutions and the very focused view on IT systems, third parties, supply chain, and cyber risk are driving regulators to mandate regulated companies to report and focus on their preparedness and ability to respond and continue to operate.

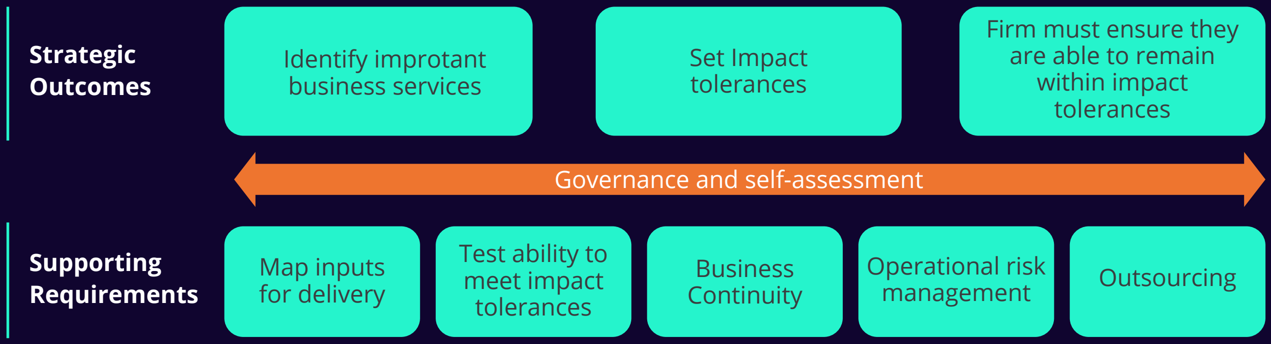
The European DORA acknowledged numerous local initiatives and looks to address the lack of detailed comprehensive rules, focusing on the particularly impacted area of digital and cyber threats and associated IT third-party risk including the lack of effective cross-border focus, internet in European banking.

"It is therefore necessary to put in place a detailed and comprehensive framework on digital operational resilience for EU financial entities. This framework will deepen the digital risk management dimension of the Single Rulebook. In particular, it will enhance and streamline the financial entities' conduct of ICT risk management, establish a thorough testing of ICT systems, increase supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities, as well as introduce powers for financial supervisors to oversee risks stemming from financial entities' dependency on ICT third-party service providers. The proposal will create a consistent incident reporting mechanism that will help reduce administrative burdens for financial entities and strengthen supervisory effectiveness".

So, What is Required?

Looking at the joint consultation document on operational resilience from the Bank of England, the PRA, and the Financial Conduct Authority (FCA), expected compliance will require the following:

Figure 1: The relationship between the PRA's operational resilience policy with other key areas of the PRA's regulatory framework



Strategic Outcomes

Identify improtant business services

Set Impact tolerances

Firm must ensure they are able to remain within impact tolerances

Governance and self-assessment

Supporting Requirements

Map inputs for delivery

Test ability to meet impact tolerances

Business Continuity

Operational risk management

Outsourcing

The framework of: identifying important business services; setting imact tolerances; and taking actions to be able to remain within impact tolerances set the strategic direction that the PRA expect firms to take. To achive the strategy, firms must:

- Map resources;
- Test their ability to remain within impact tolerances;
- Implement BCP requirements;
- Implement operational risk management requirements; and
- Implement outsourcing requirements.

Governance is an inherent part of each of the above elements, and self-assessment looks at how all of these elements combine to build the resilience of a firm.

The Section 5 of PRA Document Building Operational Resilience Impact Tolerances for important business services states:

"...mapping should enable firms and FMIs to deliver the following outcomes:

i identify vulnerabilities in delivery of important business services within an impact tolerance; and

ii test their ability to remain within impact tolerances."

This aligns to most current business continuity management programs and GRC solutions but needs to align also to the strategic business objectives and cannot be taken in isolation from standard **operational risk management.**

a Operational Risk Management

The published policy in Section 3 aligns with this observation:

"3.1 ***Operational risk management*** *supports both operational resilience and financial resilience. Firms should have* ***effective risk management systems*** *in place to manage* ***operational risks that are integrated into their organizational structures and decision-making processes.***

3.2 When assessing a firm's operational risk management, the PRA considers the extent to which firms: have reduced the likelihood of operational incidents occurring; can limit losses in the event of severe business disruption; and whether they hold sufficient capital to mitigate the impact when operational risks crystallise.

3.3 The additional requirements the PRA's operational resilience policy places on firms to limit the impact of disruptions when they occur, whatever their cause, develops the PRA's approach to operational risk in two key ways: 7 Directive 2013/36/EU (Article 85(1)).

- *it increases firms' focus on their ability to respond to and recover from disruptions, assuming failures will occur; and*
- *it addresses the risk that firms may not necessarily consider the public interest when making investment decisions to build their operational resilience. The PRA's operational resilience policy requires firms to take action so they are able to provide their important business services within their impact tolerances through severe but plausible disruptions."*

As such, the requirement for a strong operational risk management solution with fully integrated loss/risk event management, which in turn fully integrates with an organization's business impact assessments from their business continuity management system is essential. This requires a fully integrated risk management platform that measures KRI's and metrics to manage and define triggered workflows and business rules around defined tolerances.

As reviewed above, the specific regional requirements are evolving at a great pace and the requirement has been accelerated by the pandemic due to the increased risks. The huge increase in digitization was well underway before the pandemic and the personal data security requirements around the General Data Protection Regulation (GDPR) then accentuated by open banking requirements hit new levels as everyone turned to working from home, substantially increasing the attack surface.

Risks to the supply chain suddenly became very visible and whereas the IT risk of third parties had been already a strong focus since the target loss of credit card data through a third-party facilities management company and many other similar incidents.

So, do organizations simply have to just relook at their business continuity management planning, critical event planning, and align their third-party supply chain risk management?

As Baloo in the Disney version of Kipling's The Jungle Book might say… these are the "Bear Necessities", but more is required.

b Business Continuity Management (BCM)

Most organizations already have a business continuity planning function. They need to continually perform risk assessments, disaster tracking, perform scenario exercises, and look at recovery management and emergency mass communications to staff and customers and even third parties and possibly regulators.

There are many widely accepted business continuity standards and frameworks across industry sectors. Plans need to include data integration capabilities, as well as mobile-enabled access to continuity plans and crisis reports (both online and offline) to ensure rapid response times during crises.

BCM managers should proactively plan crisis responses, periodically test recovery procedures, and enable rapid recovery from disruptive incidents affecting business operations.

Critical system failures may be engineered out, but again organizations need to contemplate regulatory compliance. In a recent incident, a MetricStream customer had a full secondary data center up and running within 24 hours of a complete primary data center outage. They were about to open up to resume trading but were immediately halted by the chief compliance officer who pointed out that they could not operate as they had no back-up given that the primary data center was down and so could not legally trade. The only solution was to ensure and build a tertiary data center.

It is clearly essential that BCM plans include direct links to the third-party / supply chain risk management.

C

Third-Party & Supply Chain Risk Management (TPRM)

Typically, the key problem with third and fourth parties is the quality and reliability of data. Automatic integration of survey responses certainly helps populate the data and acts as a check-box exercise, but how can organizations improve the quality and assurance around their supply chain. In the BFSI industry, there's a clear need to closely monitor sanctions, AML to onboarding suppliers as well as customers, and integrate with Know Your Supplier resources including attention to anti-bribery and corruption.

This is also becoming of increasing focus to be able to affirm ESG status and protect against potential consequential reputational risk exposure.

Ease of use by the third parties and the addition of audits are essential components to ensure data quality and wherever possible and appropriate data and intelligence integration.

As with BCM above, an annual review for a critical supplier, such as the data center provider needs an increased cadence from the annual survey response, given the alarming speed and rate at which a business can be seen to suddenly fail. In such an event, organizations must have pre-determined what pending impacts it could have on their business to continue to operate.

d Linking BCM and TPRM

Firstly, organizations need to align and bring the processes, associated risks, controls, assets, and policies together on an aligned platform, to be readily and intelligently view and understand the interdependencies. These should also ideally link to their regulations, standards, and business objectives.

Materiality is the core focus, as organizations need to survive and sustain operations as a profitable ongoing business.

They also need to consider not just the impact of the directly related third and fourth parties, but also the potential impact to those third parties and the broader market. This could prove to be an enforcement challenge but also aligns to Corporate Social Responsibility (CSR) and ESG requirements.

Organizations will need to look at appropriate scenario analysis and predictive future outcomes. The Threat and Vulnerabilities Matrix already applied to the cyber risk assessment will need to be extended to broader operational risks and business processes.

Operational resilience is more than just business continuity and critical event planning and throws up the question of the current and forward-looking status rather than a reflection back on past data.

Managing the Data

The strategic business objectives and risk appetite of companies will always have the overarching focus to deliver returns to the investors by means of profitability. The cost of compliance has always to be measured against impact and materiality, including ensuing reputational risk arising from non-compliance or litigation. These increasing demands place the compliance officer in a difficult position, where budget is not forthcoming and yet the only way to manage the ever-increasing demands is to increase coverage and data gathering. Not surprisingly, the latest addition to compliance teams has become the data science officer.

Data exists in so many different places and with differing reliability and parameters across multiple systems. Big data analysis has evolved considerably to assist this process and needs to be fully embraced. Obtaining a “golden copy” of the right data requires an initial review and understanding of the different qualities of data around timeliness, accuracy, and confidence against which normalization rules can be drawn. Reliance on these associated data normalization algorithms however carries its own risk. This must be mitigated in the same manner as trading “Models” under MiFID II and subject to the same scrutiny audit and testing as traditional Model Risk Management under TRIM, SEC, and BofE 4 principles to give assurance around those algorithms to ensure they are relevant and still working and reliable as the business and markets change.

As such, to have any ability to look forward, the board must first have a current view of the key business risks and threats and their potential impact on a current position basis. This can only be achieved by a process of continuous monitoring. Continuous monitoring in turn needs automation that is embedded in your workflow analysis and reporting platform.

Though this sounds quite a simple task for the deployment of data analytics coupled with data integration and automation, organizations seem to struggle to access and normalize the data in a consistent and meaningful manner and many have looked to adopt internal bespoke solutions. This DIY approach is attributed to the significant cost with little if any perceived return. This may account for the Thomson Reuters report citing that less than 25% of Global Significant Important Financial Institutions (G-SIFI) have even engaged in any form of machine learning and controls automation, to deliver such assurance, with only a few of these projects completed and very few delivering value returns.

Market moving surprise critical events such as COVID-19 and the frequency of low assessed likelihood, but extremely high impact events materializing against forecast expectation, need to be managed by clear and informed decision making “from the top” using reliable up to date data.

a

Data Quality and Continuous Controls Testing

Without continuous control monitoring, this is always going to be limited to a historical point in time when the last assessment was made.

The picture then becomes clear. Organizations cannot be expected to operate and make informed decisions to maintain a state of assurance regarding the enterprise operational efficiency, without employing automation in their underlying systems. Automation of controls testing itself is not enough. Organizations need to know that the data being analyzed and tested is both the right data and normalized across the multiple siloes so that it can correctly be aggregated and deliver intelligent, concise, and clear results.

The normalization and de-duplication of multiple data sets to deliver a single source of truth is a well-established challenge in the large UK investment banks. Millions of pounds have been spent on data lakes and data scientists to use both rudimentary and more advanced federated machine learning techniques to validate the single source of data that they then need to test against controls and associated risk or threat to the key strategic business objectives.

With large investment, getting the data and even wrapping around some basic automated testing of controls around that data is being achieved, but is still costly. It needs to integrate into a reliable single source of truth into an integrated risk management platform for appropriate treatment and alignment against the framework. In this area, MetricStream has successfully integrated several continuous controls software vendor solutions, such as Continube, to great effect.

Natural language processing techniques and sentiment analysis to add further augmented decision-making suggestions for informed decision making. “So, what?” one may ask. The challenge is to obtain simple insightful results by tackling the integration of departmentalized siloed and frequently duplicated data.

For the data extraction and analysis to be effective, organizations need to pull the data into a centralized system. If that platform is driven by the data analytics solution itself, the onward application of business rules of the testing results and threshold breach issues and actions now truly starts to add value.

The required analytic capability should ideally be fully embedded into the GRC software platform such that data extraction, normalization, analysis, and machine-learned predictive notifiers are a true Value Creation enabler.

By pulling the right data seamlessly, easily, and cost-efficiently into a simple central platform with integrated manual and automated processes derived from automated testing and manual testing reviewed with transparency and easy reporting across all three lines of defense, organizations can get to a state of near real-time understanding of the present state, against which they will be able to better review and reflect on the bigger issue of operational resilience.

The board and risk committee will now be better informed on the current status, Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), and potential threats. These need to span the internal operations and assessments made internally regarding market, liquidity, and credit risk in addition to non-financial risk. In addition, organizations today need to find additional resources for horizon scanning. In a speech, Megan Butler, Executive Director of Supervision: Investment, Wholesale and Specialist, FCA, said:

“Operational resilience is not about protecting the reputation of your firms or the reputation of the industry as a whole. It is about preventing operational incidents from impacting consumers, financial markets and the UK financial system”.

For consumers - ESG concerns will undoubtedly soon additionally feature in the considerations of impacting consumers above, as well as "fair-treatment" without discriminatory approach to those identified as vulnerable (albeit through gambling addiction, history of bad debt, health and age, dementia, or other mental or physical conditions).

In relation to Financial Market impact - Reputational risk impact and concentration risks need a new additional thematic approach when considering the broader impact of a key risk event or incident, in addition to the consideration of geopolitical risks on a broader aspect than just your own organization.

And as regards the impact on the broader UK Financial system - Organizations will need to draw on specialist subject matter experts be they internal economists or consultants brought in externally.

The Integrated Risk Management Platform

To get to this position, organizations can only make informed decisions if they have a view of the current state. Scenario analysis, machine learning, and predictive analytics can leverage the data, but ultimately, they need a clear and defined integrated risk platform to span the organization, across the multiple functions and regions, products, and segments, aggregating to a single source of truth.

What does that ultimate integrated risk management platform architecture look like?

It is noteworthy that MetricStream's Seven Pillars closely align to John Wheler's deliverables view above.

Seven Pillars of the Ultimate

MetricStream Platform

Thrive on Risk

Multi-Dimensional Organization Structure
To keep up with your changing enterprise organization

APIs & Connectors
GRC-speicifc API's & Connectors to intergrate with your systems of record

Configurability
To meet your specific business needs (while protecting your upgradeability)

Federated GRC Data Model
To bind together your core GRC Libraries

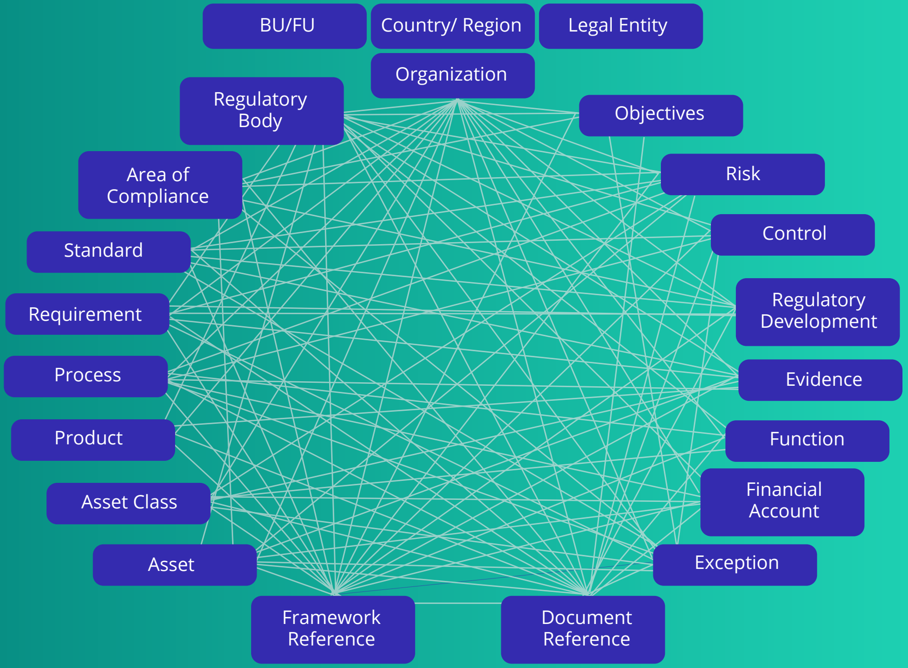
AI, ML
To automate your GRC processes

Integrated Firstline Engagement
To support your frontline and integrate into your systems of engagement

Modern, Cloud Architecture
Secure, private, modern, low-cost

- **Federated Data Model:** It is essential to be able to build multiple complex hierarchical relationships between the core libraries. In this way, clear links between business objectives, processes, risks, controls, regulatory bodies, and regulations can be created in a multi-dimensional form that aligns with the business, however complex. This one-to-one, one-to-many, many-to-many relationships transform "complexity" into "simplicity" and allow for clear and insightful data to be drawn together across the organization.

Leveraging The Power of Integrated Data Model



Relational data objects with a federated architecture

Reduced redundancy and improved accountability due to defined relationships

Many to Many relationships between multiple data objects

Data objects stored in structured libraries with ease of access

These data libraries, however, also ensure conformity and standardization across the enterprise. Many frameworks in place across organizations have become fragmented and misaligned. Great operational benefits can be gained from a review of the global framework, to simplify and align with the “Tone from the Top” approach on key business objectives with the associated key risks and key controls related. Classifying and defining more granular risks in hierarchies allows for simpler and easier risk aggregation and a true visible understanding of risk, by the focus on clearly defined risk and controls frameworks.

- **Multi-Dimensional Organizational Structure:** The ability to manage a complex hierarchy that can readily add or remove the geographical and functional segmentation as required is crucial to holistically view the state of risks, controls, and processes across the enterprise through the most appropriate lens. A MetricStream customer underwent transformational organizational structure change from a more traditional hierarchy to a “Spotify model” of quads, tribes, chapters, and guilds. The ability to retain the data and simply adapt the structure can pay huge dividends here and is, in this instance, simply achieved through associated API scripting.

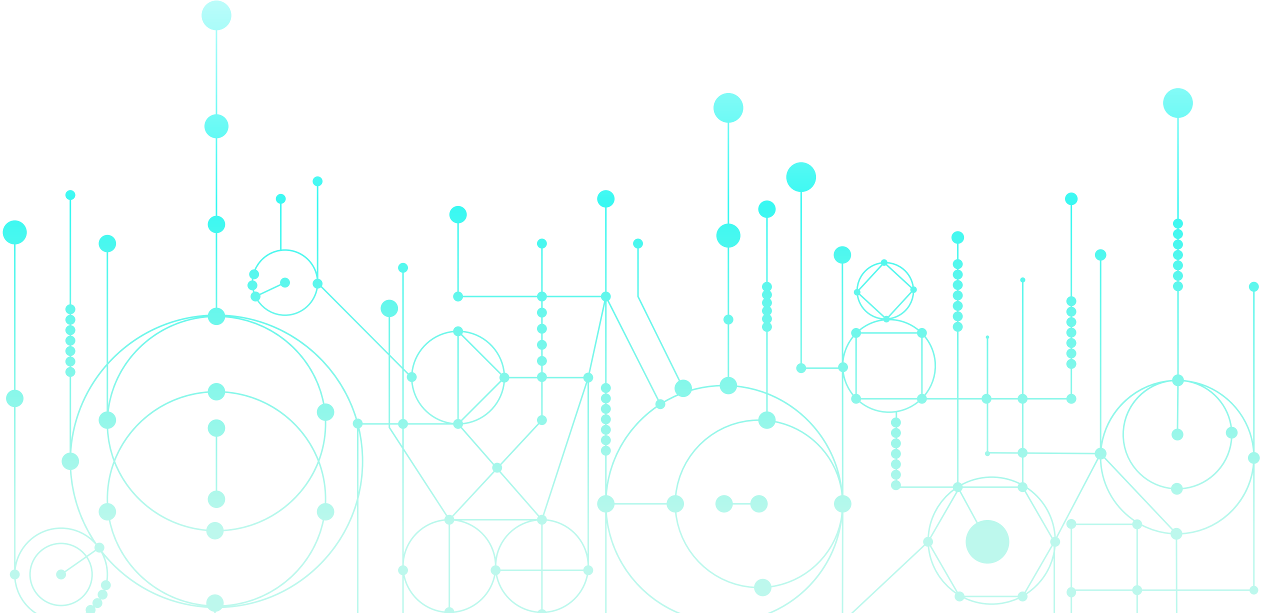
- **AI/ML:** Both the PRA and FCA have openly stated that the velocity and increase of data in terms of the attack surface, regulations, and compliance necessitate an embracing of innovation and technology in order to simply keep pace and manage the cost of compliance. Natural language processing is essential for contextualized search. Many are wary of the use of artificial intelligence and promote the adoption of augmented decision-making where it is possible to humanly check the automated, suggested action before blindly relying on machine interpretation. The removal of random sampling, however, to use machine learning and AI to detect anomalies and patterns across the whole population data set, substantially improves assurance and will remove the sampling error risk. There is, however, the added mandate to audit and test all ML and AI models, which should extend to an organization’s controls testing automation models and not simply their trading applications as under MiFID II.

- **API’s and Connectors:** It is far too onerous to look to have an integrated risk management platform that inputs all the data from across the enterprise in one big data database. The data already exists across the enterprise and so needs to be analyzed for the “single source of truth” or acceptable normalized version of truth, that is reported to the IRM platform. So peaceful co-existence with ERP and applications across the organization is essential. These need to be readily adaptable to the numerous and frequent software and security changes and ensure strong information security protection against such risks as experienced with the recent SolarWinds incident.

- **Integrated First Line Engagement:** For the success of any attempt to view the status of operational resilience or level of risk across the enterprise, any solution is only ever as good as the data input. The prime source of data has to come from the risk and control owners, namely the first line. At the coalface, it is important the user experience to report a loss, near miss, control failure, or new emerging risk is as simple and easy as possible and expressed in simple human language terms without jargon or subject matter expert (SME) intervention. By capturing the data as a chat or question, AI and ML have a great function in triaging the simplified data capture from the first line reporting, pre-contextualized for SME review and treatment. User adoption is the biggest factor attributed to the failure of GRC projects’ successful return on investment (ROI) and is crucial to success. Without good data input, any solution will have limited value in visualizing your status of operational resilience.

- **Configurability:** Similar to first line adoption and MDOS above, no organization is the same. Culture and processes will be as different as the people within organizations. It is true to say, however, that peers in a specific market sector will have largely the same business objectives, risks, controls, policies, procedures, and regulations. Configuration, meaning small changes such as changing field names and minor workflow changes, all fit into a no-coding simple configuration change. Powerful “App Studio” tools are recommended to assist and enable configuration and, at all costs and avoid solution customization that requires specific additional coding. This creates a deviation from the standard solution and causes tremendous future upgrade risks and extensive regression testing and adjustments are likely to be required that can impact performance and future access to feature enhancements, without incurring bespoke fees for each change. Organizations must drive their provider to develop the required design as a new feature in the upgrade program to ensure it will be seamlessly supported once released in the product solution as standard. Bleeding edge in these cases can lead to isolated and unsupported complications in the future and where product community engagement is actively encouraged to ensure the solution evolves in line with the broad consensus user requirements of the market segment.

- **Modern Cloud Architecture:** In today's world, AWS, Azure, and Google have cornered the market for secure, distributed, low-cost, high-performance solutions that in themselves deliver an in-built operational resilience of architecture by design. Security must not be compromised and the reliance on a single vendor adds a level of risk that needs to be added into the appetite assessment to consider back-up in a different cloud provider as a standard third-party risk assessment. Leveraging the cloud provider ecosystem will enable further data and application integration and innovation and assist in future-proofing the value of investment.



Quantification of Risk

Quantification of risk, especially cyber risk, becomes ever more important as organizations need to be able to determine an acceptable appetite and better assess true critical impact.

More and more, the accepted view of risk as a weighted score derived from impact vs likelihood, mitigated by the effectiveness of controls, to derive a residual risk score is failing to get the visibility of the decision-makers, who are often lacking in detailed subject matter expertise. The most cited area is that of cyber, digital, and information security risk. To bring this into real perspective and focus of the board and key decision-makers, organizations now need to pay far more detailed attention to quantified risk assessment.

In the cyber risk arena, there are pre-existing vulnerability software scanners acting in real-time from such software vendors as Qualys, Tenable, etc. By aligning the integrated data results in a Threat and Vulnerabilities Matrix, organizations can gain the ability to pull this data to readily perform a detailed data-driven cyber risk assessment and derive a quantifiable risk exposure value that has an immensely powerful impact on decision making.

Scenario Analysis Workflow

To further explore the consequential reputational risk and similar inter-related risks, it is becoming essential also to adopt a scenario analysis process to discern and determine the risk assessment of many risks to gain a better understanding of acceptable tolerance levels and to align with the acceptable/stated risk appetite.

Summary & Conclusion:

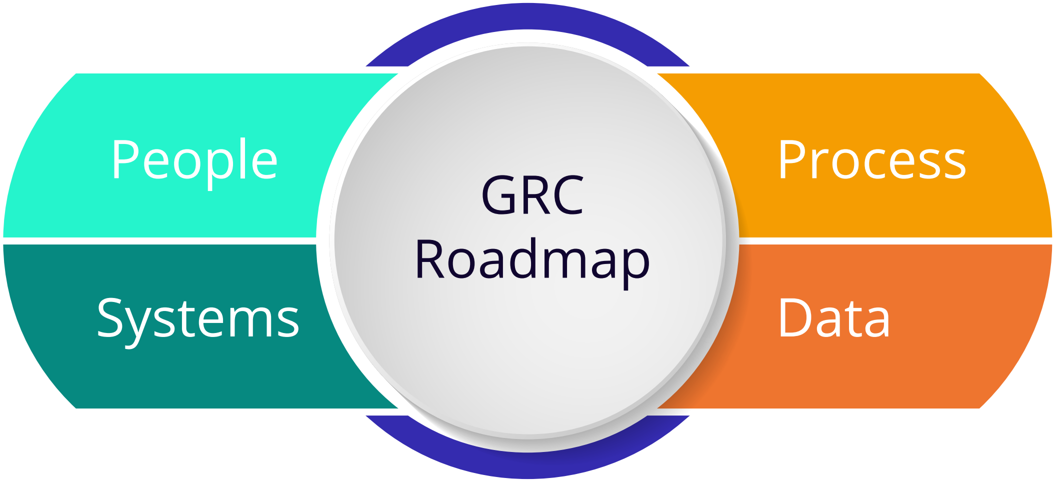
To be able to readily view the enterprise status of operational resilience, organizations need to focus on people, processes, systems, and data.

To pull these effectively together, they need a simplified clear vision and adaptable risk and controls framework that can adapt and change with innovation and ever-changing regulations and standards pulled together across all three lines on a powerful integrated risk management platform.

With limited budgets and core business objective focus, organizations must therefore find a way to be agile and to do more with much less!

Ultimately the value must readily be drawn back to the strategic business objectives. For most organizations (though not all our NGO customers), profit is the key driver.

The status of operational resilience relates directly back to that focus to achieve both profitability and sustainability.



The correct treatment of the governance, risk and compliance (GRC) delivers the real value benefits through an integrated risk platform that has the underlying maturity and complexity to deliver simple and actionable data reporting from across the organization.

Complexity here relates to the need for the solution to have the depth and maturity to handle such issues as multi-currency loss events aligned to the 7 Basel II categories and the structured interrelationships between processes, entities, functions, assets, and products that may be lacking from some solutions.

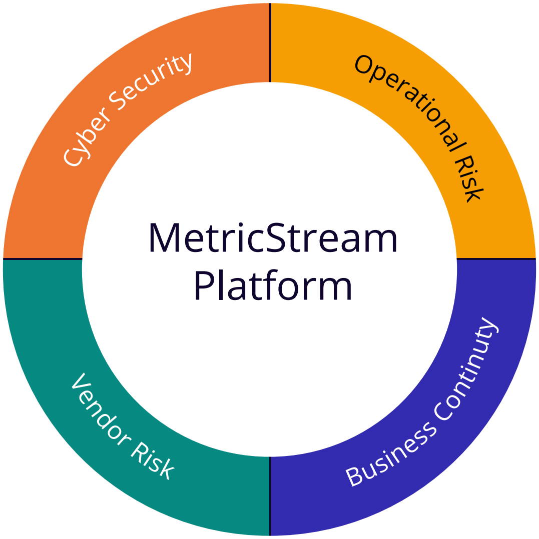
Essential requirements include the need for **operational risk management including loss/risk event route cause analysis, business continuity management,** and **third-party management**. Additional and specific focus should be driven towards the **information security and cyber risk management** and impact to **assets, systems**, and **processes** across the enterprise.

This may sound too simplistic. However, by employing data integration, automation, freeing up resources, and taking away the mundane processes (and yet making them more efficient and including greater coverage and greater assurance), organizations can free up time for specialist subject matter risk and compliance teams to focus on these more complex macro-risk ideals coming down from the regulators.

It is essential that organizations deliver an increased assurance and transparency of their current status concerning residual risks to the strategic business objectives, to which the ability to view and report the status of operational resilience will be clearly evidenced.

Decision-making needs to be made from reliable, up-to-date information. The leadership team can have confidence that the key decisions they are being tasked to make (and held with ever more personal accountability) are made from being able to truly have ***a finger on the pulse*** of the organization's state of health and status of operational resilience. With this enhanced knowledge, your organization will therefore be better positioned to thrive on risk.

MetricStream Solution for Operational Resilience



IT Risk and Control Assessments
Threat & Vulnerability
Cyber Risk Quantification

Risk & Control Assessment
Loss Data management
Keys Metrics
Issue & Remediation
Risk Analytics & Reporting

Vendor Information Management
Onboarding & Due Diligence
Continuous Vendor Monitoring

Business Impact Analysis
Business Continuity Planning
Emergency & Crisis Management
Disaster Recovery management

MetricStream Platform

GRC Cloud | GRC Foundation | GRCIntelligence | Analytics | AppStudio

CONTACT US | REQUEST A DEMO

Email: info@metricstream.com

metricstream