July 2024

Risk & Resilience Management by Design

360° Visibility into Risk & Resilience Management

Sponsored by:

STRATEGY***PERSPECTIVE***

Governance, Risk Management &

Table of Contents

The Need for Contextual Awareness of Risk & Resilience 4
- Dynamic, Disrupted & Distributed Business is Difficult to Control 4
- Understanding the Interrelationship of Risk and its Impact on Operations 5
- Providing 360° Contextual Awareness of Risk and Resilience 8
  - *The Risk & Resilience Central Nervous System 9*

Risk & Resilience Management by Design 11
- 360° Visibility into Risk & Resilience Management 11
- Risk & Resilience Management Strategic Plan 12
- Risk and Resilience Management Architecture 13
  - *Risk and Resilience Management Process Architecture 14*
  - *Risk and Resilience Management Information & Technology Architecture 21*
- Building a Business Case for Risk & Resilience Management 25

GRC 20/20's Final Perspective 27
- Growing in Risk & Resilience Management Maturity 27

About GRC 20/20 Research, LLC 30

Research Methodology 30

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

Risk & Resilience Management by Design

360° Visibility into Risk & Resilience Management

The Need for Contextual Awareness of Risk & Resilience

Dynamic, Disrupted & Distributed Business is Difficult to Control

Organizations take risks but fail to monitor and manage these risks effectively in an environment that demands risk agility and resilience. Too often, risk management is seen as a compliance exercise and not truly integrated with the organization's strategy, decision-making, and objectives. A cavalier approach to risk-taking results in the inevitable failure of risk management, providing case studies for future generations on how poor risk management leads to the demise of organizations - even those with strong brands.

Gone are the years of simplicity in business operations. Exponential growth and change in risks, regulations, globalization, distributed operations, competitive velocity, technology, and business data encumber organizations of all sizes. Keeping these changes and their impact on business strategy, operations, and processes in sync is a significant challenge. Organizations must see the intricate relationships and impacts of risks on objectives and processes. They need full contextual awareness of risk and resilience.

The complexity of business—combined with the intricacy and interconnectedness of risk and business objectives—necessitates implementing a strategic and integrated approach to risk and resilience management. This includes a top-down enterprise view of risk aligned with objectives and a bottom-up operational understanding of risk within the organization's processes and relationships.

Over the past few years, organizations have seen lots of disruption to objectives. It has been a risk and resilience rollercoaster. Some industries and organizations have failed, while others held firm and navigated risk events with agility. But there are lessons to be learned. These include:

- **Interconnected risk.** Organizations face an interconnected risk environment; risk and resilience cannot be managed in isolation. The organization needs to see across silos of risk management to see complex relationships of risk on objectives.

- **Dynamic and agile business.** The organization needs to be agile in a changing risk environment. It must adapt objectives and seize opportunities while ensuring risk is managed within limits to those objectives. The organization needs to react

quickly to stay in business. Organizations are constantly in flux as distributed business operations and relationships grow and change. At the same time, the organization is trying to remain competitive with fluctuating strategies, technologies, and processes while keeping pace with change to risk. The multiplicity of risk environments that organizations must monitor spans strategic, regulatory, geopolitical, market, credit, and operational risks. Managing risk and business change on numerous fronts buries the organization when managed in silos.

- **Operational intelligence.** Risk and resilience management, done correctly, requires a detailed and intimate understanding of how the business operates and how it breaks. Only with this intelligence can the organization manage uncertainty in the context of the business achieving its objectives. This has taught organizations that risk management requires a 360° view of objectives, risks, processes, and services within the organization and the extended enterprise.

- **Disruption.** International and local events easily disrupt business. Organizations have had to respond to disruptions, geo-political risk, unrest, economic uncertainty, inflation, commodity availability, competitive shifts, changes in business models, shifting regulations, environmental disasters, cyber risk, and more. Organizations face a complex, chaotic, and even hostile risk environment while attempting to manage high volumes of structured and unstructured risk data across multiple systems, processes, and relationships to see the big picture of performance, risk, and resiliency. The velocity, variety, veracity, and volume of risk data is overwhelming, disrupting the organization and slowing it down at a time when it needs to be agile and fast.

- **Dependency on others.** No organization is an island; the modern organization is the extended enterprise. Even the smallest of organizations can have distributed operations complicated by a web of global relationships. The traditional brick-and-mortar business with physical buildings and conventional employees has been replaced with an interconnected mesh of relationships and interactions that now define the organization. Complexity grows as these interconnected relationships, processes, and systems nest themselves in intricacy. This requires the organization to manage and monitor risk and resilience in third-party relationships.

- **Risk ownership and accountability.** There is a growing awareness among executives and directors that risk management needs to be taken seriously. Oversighting risk management as an integrated part of business strategy and execution is part of their fiduciary obligations.

Understanding the Interrelationship of Risk and its Impact on Operations

Risk management is often misunderstood, misapplied, and misinterpreted due to scattered and uncoordinated approaches that get in the way of sharing data. Various departments manage risk with different approaches, models, requirements, and perspectives on risk and how it should be measured and managed. Risk management silos — where distributed business units and processes maintain their own data,

spreadsheets, analytics, modeling, frameworks, and assumptions — pose a significant challenge for enterprise risk visibility and fails to provide actual value to the business in pursuit of objectives. Documents and spreadsheets are not equipped to capture the complex interrelationships that span global operations, business relationships, lines of business, and processes. Individual business areas focus on their view of risk, not the aggregate picture, and cannot recognize substantial and preventable losses. When an organization approaches risk in scattered silos that do not collaborate, there is little opportunity to be intelligent about risk.

A siloed approach to risk management fails to deliver insight and context and makes it nearly impossible to connect risk management and decision-making, business strategy, objectives, and performance. This is because risk intersects, compounds, and interrelates with other risk areas to create a more significant risk exposure than each silo is independently aware of. Today, it is critical that all these roles work off the same data and that this risk data is clean, reliable, timely, and thus actionable and meaningful.

Keeping risk, complexity, and change in sync is a challenge not only when risk management is buried in the depths of departments but also when risk management is approached as a compliance or audit function and not as an integrated discipline of decision-making that has a symbiotic relationship with performance and strategy. Unfortunately, risk management is only an expanded view of routine financial controls for some organizations, resulting in nothing more than a deeper look into internal controls with some heat maps thrown in. It does not truly provide an enterprise view of risk aligned with strategy and objectives. Completing a risk assessment process and ticking the box has gotten in the way of proper risk analysis and understanding.

ISO 31000 defines risk as the effect of uncertainty on objectives. Risk management is about managing uncertainty. Organizations need to link and measure risk to strategic objectives. Good risk management results in improved decision-making and fewer surprises when achieving the organization's objectives.

Today's organization needs to be agile in managing risk and its impact on the organization's objectives from the moment it is developing on the horizon, as well as resilient in recovering from risk events when they materialize. Organizations need to understand how to monitor risk-taking, measure whether the associated risks are the right risks to achieve objectives, and review whether the risks are managed effectively to ensure the organization's agility and resilience. Amidst this uncertainty, effectively managing risk and building resilience has become imperative for organizational success.

To manage risk effectively, organizations must adopt a holistic approach encompassing a top-down strategic view aligned with objectives and a bottom-up operational perspective embedded within processes and activities. This aligns with the OCEG definition of GRC where "GRC is a capability to reliably achieve objectives [GOVERNANCE], address uncertainty [RISK MANAGEMENT], and act with integrity [COMPLIANCE]."[1]

1 *For more information on the official definition of GRC and the GRC Capbility Model, please visit www.OCEG.org*

However, the modern organization faces many challenges in addressing an integrated risk and resilience management approach. These include:

1. **Lack of risk agility.** Organizations often struggle to respond promptly to emerging risks due to rigid processes and hierarchies. Failure to adapt quickly to changing circumstances can lead to missed opportunities or unanticipated threats.

2. **Fragmented and inaccurate risk data.** Siloed data across disparate systems makes obtaining a comprehensive view of risks challenging. Inaccurate or outdated data undermines the reliability of risk assessments and decision-making processes.

3. **Limited visibility.** Limited visibility into interconnected risks and dependencies hampers the ability to anticipate and mitigate potential impacts. Organizations are vulnerable to cascading failures without a clear understanding of the entire risk landscape.

4. **Inefficient manual processes for risk management.** Manual and disjointed risk management processes result in inefficiencies and delays. Hundreds or thousands of out-of-sync documents, spreadsheets, and emails encumber these. The lack of automation and standardized workflows impedes timely identification and response to risks.

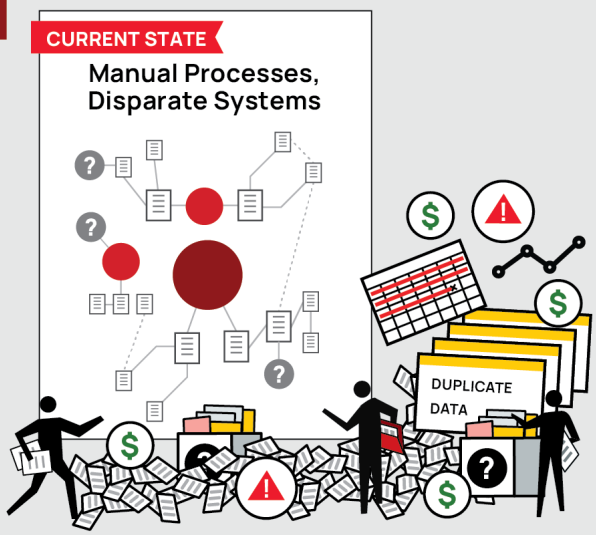
5. **Inadequate risk reporting.** Traditional risk reporting methods often fail to provide actionable insights or meaningful context. Poorly structured reports obscure critical risk information and hinder informed decision-making.

6. **Limited scalability.** Scalability challenges arise when existing risk management practices cannot accommodate growth or organizational changes. Scaling risk

Top 10 Challenges Companies Face

Managing risk and resilience in manual processes poses many challenges for companies:

- Lack of Risk Agility
- Fragmented & Inaccurate Data
- Limited Visibility
- Inefficient Workflows
- Inadequate Risk Reporting
- Limited Scalability
- Resource Intensiveness
- Ineffective Collaboration
- Resilience Planning Gaps
- Difficulties in Change Management



Address these challenges by transitioning to an integrated risk and resilience management solution that provides a unified view of data, streamline workflows, and deliver greater efficiency, effectiveness, resilience, and agility to the organization.

management efforts across multiple business units or geographies becomes increasingly complex.

7. **Resource intensiveness.** Resource constraints, both in terms of personnel and technology, hinder effective risk management efforts. Limited resources result in suboptimal risk mitigation strategies and increased vulnerability. Too often, GRC 20/20 hears that 80% of risk staff time is spent managing documents, spreadsheets, and emails rather than managing risk.

8. **Ineffective collaboration.** Siloed organizational structures and cultural barriers inhibit collaboration and information sharing. Lack of cross-functional collaboration undermines the ability to identify and address systemic risks.

9. **Resilience planning gaps.** Inadequate focus on resilience planning leaves organizations vulnerable to disruptions. Failure to anticipate and prepare for potential risk events can lead to significant operational disruptions and financial losses.

10. **Difficulties in business change management.** Resistance to change and organizational inertia pose challenges to keeping risk current as the business continuously evolves.

Providing 360° Contextual Awareness of Risk and Resilience

To address these challenges, organizations must transition to integrating risk and resilience management as part of a broader GRC strategy. This function should be focused on enabling the organization to reliably achieve objectives amid risk and uncertainty. This requires a unified view of risk information and processes that deliver greater efficiency, effectiveness, resilience, and agility. By centralizing risk management functions and integrating risk accountability throughout all levels of the organization, organizations can achieve a more holistic understanding of risks and opportunities.

The physicist Fritjof Capra made an insightful observation on living organisms and ecosystems that rings true when applied to risk and resilience management:

"The more we study the major problems of our time, the more we come to realize that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent."

Capra's point is that ecosystems are complex and interconnected and require a holistic understanding of the intricacy of interrelationships as an integrated whole rather than a dissociated collection of parts. Change in one segment of an ecosystem has cascading effects and impacts the entire ecosystem. Organizations need 360° situational awareness and visibility of their processes, operations, objectives, and risks.

What complicates this is the exponential effect of risk on the organization. The business operates in a world of chaos, and even a small event can cascade, develop, and influence what ends up being a significant issue. Dissociated siloed approaches to

risk and resilience management that do not span processes and systems can leave the organization with fragments of truth that fail to see the big picture across the enterprise and how it impacts its strategy and objectives. The organization needs visibility into objective and risk relationships in strategy and performance management and across business functions and processes.

The complexity of business and the interconnectedness of risk data requires that the organization implement an enterprise view of risk and resilience monitoring, automation, and enforcement that enables the business to achieve its objectives, forecast what is coming at the organization, prepare the organization to seize opportunities while mitigating loss, and manage uncertainty to minimize surprises.

Firms globally and across industries focus on taking an integrated approach to risk and resilience (historically business continuity/disaster recovery) management that is part of a broader GRC strategy. This is becoming a key regulatory requirement in many industries. Still, the value is beyond regulatory compliance as it drives operational intelligence and insight to help organizations navigate and respond to risk.

The Risk & Resilience Central Nervous System

Navigating the complex and dynamic landscape of organizational risk requires a leader with a keen sense of balance, foresight, and an ability to harmonize diverse elements. Much like a conductor who leads an orchestra through intricate compositions, a Chief Risk Officer (CRO) orchestrates the management of various risks to ensure a company's smooth operation and sustainable growth. The CRO, much like an orchestra conductor, plays a vital role in harmonizing the various types of risks in alignment with the organization's objectives. The CRO ensures that risks are managed in context. By managing uncertainty (risk) in achieving objectives, the CRO works with the business to establish appropriate risk tolerances and proactively sees risks across silos to address the complexity of interconnected uncertainties.

Delivering this requires a holistic view of the organization's objectives and processes in the context of uncertainty and risk and the symbiotic interaction of risk management and resilience. Leveraging technology solutions such as advanced analytics, artificial intelligence, and automation can enhance risk agility and enable proactive risk management strategies. Ultimately, a comprehensive risk and resilience management approach empowers organizations to navigate uncertainty with confidence, proactively prepare for potential risks, and effectively respond to disruptions when they occur.

In this context, organizations must develop a risk management capability that is aligned with strategy, performance, and objectives and operate as a risk-central nervous system. Consider the following from Steve Balmer, former CEO of Microsoft:

> **"If you think of the human body, what does our nervous system let us do? It lets us hear, see, take input. It lets us think, analyze, and plan. It lets us make decisions and communicate and take action. Every company has a nervous system: companies take inputs, they think, they plan, they communicate, they take action."**

The nervous system connects with other major systems of the body and provides, among other things, analytical capability, strategic thinking, and quick response to the environment. In the same context, organizations need a command-and-control hub with the analytical capability to measure and monitor a connected view of risk—a risk central nervous system of the business.

Managing risk and resilience effectively requires multiple inputs and methods of modeling and analyzing risk. This requires information gathering — risk intelligence — so the organization has a full perspective and can make better business decisions. The demand is for predictive analytics to extract from this mass amount of data, which will help prevent future significant losses, events, and incidents and further help strategic business objectives succeed. This enables organizations to spend more time focusing on risk analysis in the context of the organization, its strategy, and objectives. Technology makes it easier to share data while still maintaining independence of thought and action across the organization.

In light of this, organizations should consider:

- Can the organization accurately gauge risk's impact on strategy, performance, and objectives?
- How does the organization know it takes and manages risk effectively to achieve optimal operational performance and meet its strategic objectives?
- Which objectives could fail as a result of current risks?
- How does the organization ensure it makes the right business decisions?
- What impact does risk have on products and services?
- What is the impact or potential impact on customers?
- Do businesses understand the interrelationships and correlations between risks?
- Does the organization understand the relationships generally between cause and effect, processes, end-to-end process flows, and products and services?
- Does the organization understand the risk exposure to each objective or process, and how does it relate with other risks to aggregate into an enterprise risk perspective?
- Does the organization have the information to respond quickly, mitigate risk exposure, and seize opportunities?
- Does the organization monitor key risk indicators across critical projects and processes?

- Is the organization optimally measuring and modeling risk?

The Bottom Line: The goal is comprehensive, straightforward insight into risk and resilience management to identify, analyze, manage, and monitor risk in the context of the organization's objectives and how it impacts strategy, performance, operations, processes, and services. It requires the ability to continuously monitor changing contexts and capture changes in the organization's risk profile from internal and external events as they occur that can impact objectives. This enables risk agility to forecast and plan what is coming at the organization to prepare and navigate it. It also gives a detailed understanding of how the organization operates and how it breaks to ensure resilience when risk becomes a reality. Successful risk and resilience management requires the organization to provide an integrated strategy, process, information, and technology architecture.

Risk & Resilience Management by Design

360° Visibility into Risk & Resilience Management

The primary directive of a mature risk and resilience management program is to deliver effectiveness, efficiency, resilience, and agility to the business. This is in the context of managing the breadth of risks to the organization's strategy, objectives, performance, and operations. This requires a strategy that connects the enterprise, business units, processes, transactions, and information to enable transparency, discipline, and control of the ecosystem of risks across the extended enterprise.

GRC 20/20 has identified three approaches organizations can take to manage risk:

- **Anarchy – ad hoc department silos.** This is when the organization has scattered risk departments doing different yet similar things with little to no collaboration. Distributed and siloed risk management initiatives never see the big picture and fail to put risk management in the context of organizational strategy, objectives, and performance. The organization does not think big picture about how risk management processes can be designed to meet a range of needs. An ad hoc approach to risk management results in poor visibility into the organization's relationships, as there is no framework for bringing the big picture together; there is no possibility to be insightful about risk and performance. The organization fails to see the web of risk interconnectedness and its impact on performance and strategy, leading to greater exposure than any silo understood on its own.

- **Monarchy – one size fits all.** If the anarchy approach does not work, the natural reaction is the opposite: centralize everything and get everyone to work from one perspective. However, this has its issues as well. Organizations become susceptible to one department overseeing risk without fully understanding the breadth and scope of all the necessary risk management priorities at operational levels. The needs of one area may also come to overshadow the needs of others. From a technology point of view, it may force many parts of the organization to

manage risk with the lowest common denominator, resulting in watered-down risk management.

- **Federated – an integrated and collaborative approach.** The federated approach is where mature organizations find the greatest balance in a collaborative and connected view of risk management, governance, and oversight. It allows for some level of department and business function autonomy when needed but also focuses on a common risk governance model and architecture in the various groups across risk management participants. A federated approach increases the ability to connect, understand, analyze, and monitor risk interconnectedness. It mainly allows different business functions to focus on their areas while reporting to a shared risk governance framework and architecture. Different functions participate in risk management with a focus on coordination and collaboration through a common core architecture that integrates well with other systems.

Risk & Resilience Management Strategic Plan

Designing a risk and resilience management program starts with defining the strategy. The strategy connects key business functions with a common risk governance framework, ontology, and policy. The strategic plan is the foundation that enables risk accountability, discipline, and control of the risk ecosystem across the enterprise.

The core elements of the risk and resilience management strategic plan include:

- **Risk and resilience management team.** The first piece of the strategic plan is building the cross-organization risk management team (e.g., committee, group). This team needs to work with risk owners to ensure a collaborative and efficient risk governance process is in place. The goal of this group is to take the varying parts of the organization that have a vested stake in risk management and get them collaborating and working together on a regular basis. Various roles often involved on the risk and resilience management strategic team are enterprise and operational risk management, resilience teams (formerly business continuity/disaster recovery), compliance, ethics, legal, finance, information technology, security, audit, quality, health & safety, environmental, and business operations. One of the first items to determine is who chairs and leads the risk management team; this is typically the Chief Risk Officer of the organization.

- **Risk and resilience management charter.** With the initial collaboration and interaction of the risk management team in place, the next step in the strategic plan is to formalize this with a risk management charter. The charter defines the critical elements of the risk and resilience management strategy and gives it executive and board authorization; it will contain the mission and vision statement of risk and resilience management, the members of the risk and resilience management team, and defines the overall goals, objectives, resources, and expectations of risk and resilience management. The fundamental goal of the charter is to establish alignment of risk and resilience management to business objectives, performance, and strategy. The charter should also detail board oversight responsibilities and risk and resilience management reporting.

- **Risk and resilience management policy.** The next critical item to establish in the risk and resilience management strategic plan is the writing and approval of the risk and resilience management policy (and supporting policies and procedures). This sets the initial risk and resilience management structure in place by defining categories of risk, risk accountability and ownership, associated responsibilities, approvals, assessments, evaluation, assurance activities, and reporting. The policy should require an inventory of all risks to be maintained and aligned with the organization's objectives with appropriate categorizations, approvals, and identification of risks.

Risk and Resilience Management Architecture

The risk and resilience management strategy and policy are supported and operationalized through a risk and resilience management architecture. Organizations require complete situational and holistic awareness of risks across operations, processes, transactions, and data to see the big picture in the context of organizational performance and strategy. Distributed, dynamic, and disrupted business requires the organization to take a strategic approach to risk and resilience management architecture. The architecture defines how organizational processes, information, and technology are structured to make risk and resilience management effective, efficient, resilient, and agile across the organization and its relationships.

These are the three areas of the risk and resilience management architecture:

1. *Risk and resilience management process architecture*
2. *Risk and resilience management information architecture*
3. *Risk and resilience management technology architecture*

These architectural areas must be initially defined in this order. The risk and resilience management processes determine the types of risk information needed, gathered, used, and reported. The information architecture combined with the process architecture will define the organization's requirements for the risk and resilience technology architecture. Too many organizations select technology for risk management first, which in turn dictates what their risk process and information architecture will be. This forces the organization to conform to technology for risk management instead of finding the technology that best fits their risk process and information needs.

The goal of these three areas is to enable and align risk and resilience management to the business to achieve:

- **Holistic awareness of risk.** To ensure there is a defined risk taxonomy across the enterprise that structures and catalogs risk in the context of business objectives and assigns accountability. A consistent risk and resilience architecture identifies objectives, processes, services, risks, and impact tolerances. It keeps the taxonomy current - and various risk frameworks are harmonized into an integrated risk and resiliency framework. The risk information and technology

architecture discussed later aggregates risk data and effectively communicates, monitors, and manages risk.

- **Establishment of risk culture.** Risk policy must be communicated, monitored, and enforced to establish a risk management culture. Policies are kept current, reviewed, and audited on a regular basis. Risk appetite and tolerance are established and reviewed in the context of the organization's objectives and context and are continuously mapped to the organization's performance and objectives. Technology monitors key risk indicators (KRIs) to ensure the management of risk policy and the management of risk against appetite, tolerance, and capacity.

- **Risk-intelligent decision-making.** This means the business has what it needs to make risk-intelligent organizational decisions. Risk strategy is integrated with organizational strategy —an integral part of business responsibilities. Risk assessment is done in the context of business change and strategic planning and structured to complement the organization's lifecycle to help executives make effective decisions.

- **Accountability for risk and resilience.** Accountability and risk ownership are established features of risk governance and culture. Every risk, at the enterprise and business-process level, has clearly established owners. Risk is communicated to stakeholders, and the organization's track record should illustrate successful risk management and resilience against established risk tolerances and appetites.

- **Multidimensional risk and resilience analysis and planning.** The organization has a range of risk analytics, correlation, and scenario analysis tools. Various qualitative and quantitative risk analysis techniques are in place, and the organization needs an understanding of historical loss to feed into its analysis. Risk treatment plans — whether acceptance, avoidance, mitigation, or transfer — must be effective and monitored for progress.

- **Visibility of risk as it relates to performance and strategy.** The enterprise views and categorizes risk in the context of corporate optimization, performance, and strategy. KRIs are implemented and mapped to key performance indicators (KPIs). Risk indicators are assigned established thresholds and trigger relevant reporting. The risk information adheres to information quality, integrity, relevance, and timeliness.

Risk and Resilience Management Process Architecture

Risk and resilience management processes are a part and subset of overall business processes. They are used to manage and monitor the ever-changing risk environments. The risk management process architecture is the structural design of processes, including their components of inputs, processing, and outputs. This framework inventories and describes risk and resilience management processes, their components and interactions, and how they work together and with other enterprise processes.

While risk and resilience management processes can be very detailed and vary by organization and industry, there are five that organizations should have in place:

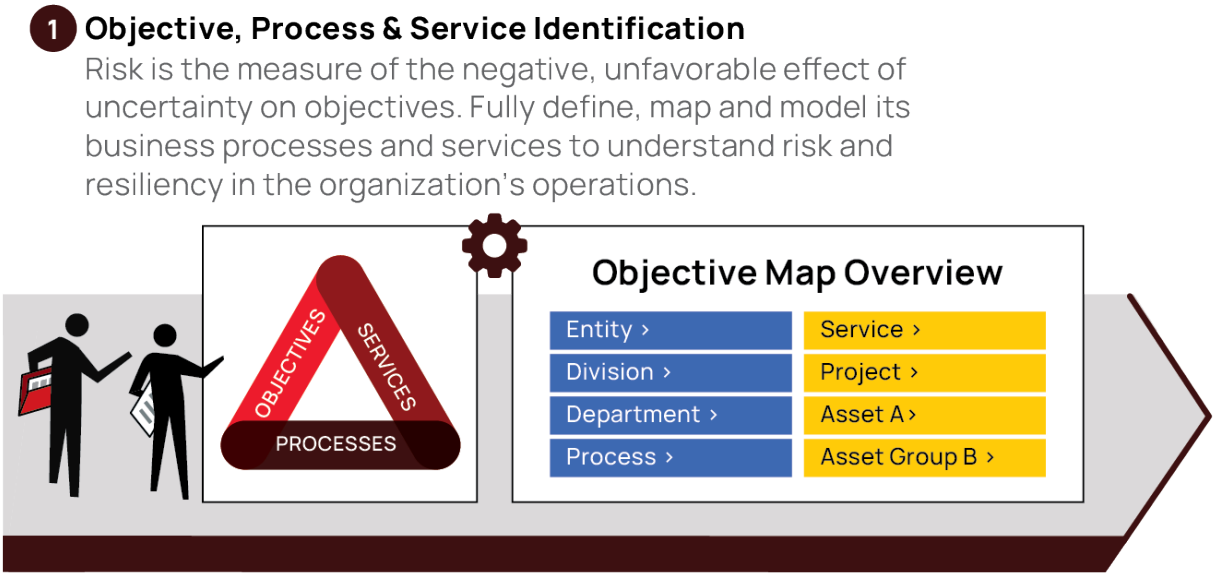
1. **Objective, process, and service identification.** Risk is the measure of the negative, unfavorable effect of uncertainty on objectives. Organizations need to fully define, map, and model their business objectives, processes, and services to understand risk and resiliency in their operations.

    - Begin by clearly defining the organization's strategic and operational objectives across various departments and functions. This includes identifying key performance indicators (KPIs) and success metrics tied to these objectives.

    - Next, thoroughly mapping and modeling the organization's business processes and services must be conducted. This involves documenting each step in the process flow and identifying dependencies, inputs, outputs, and stakeholders involved.

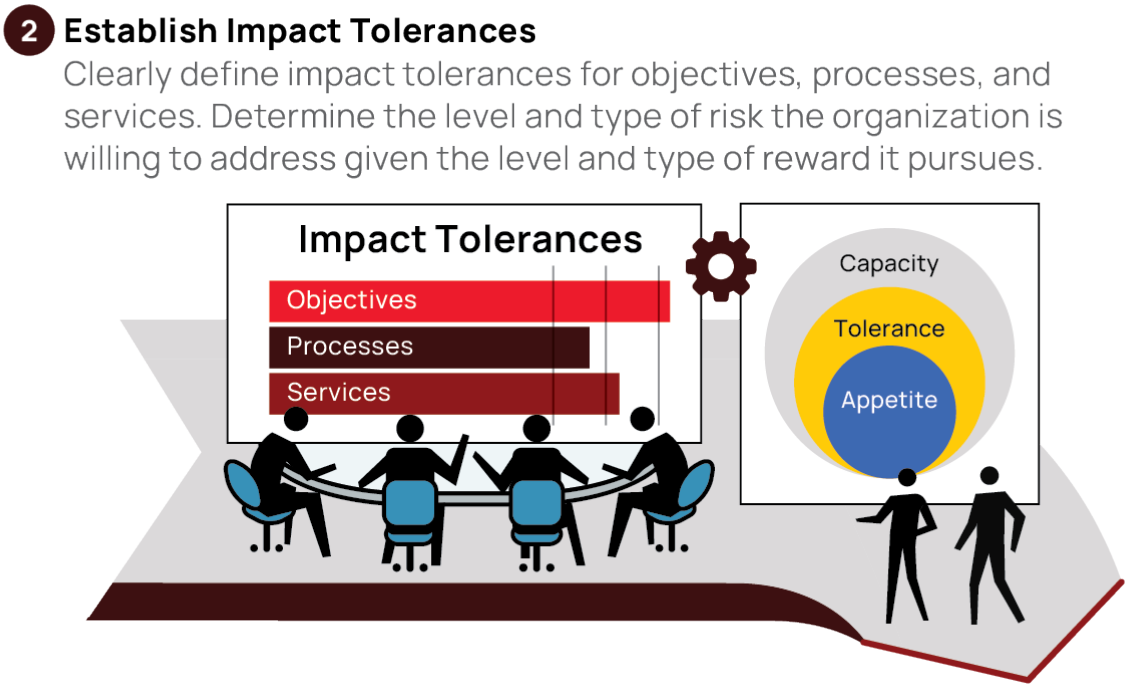
    - Utilize process modeling tools and techniques such as Business Process Model and Notation (BPMN) or Value Stream Mapping to visualize and analyze the end-to-end processes.

    - During this phase, it is crucial to assess the criticality of each process and service to the organization's operations and objectives. This helps prioritize risk management efforts and allocate resources effectively.



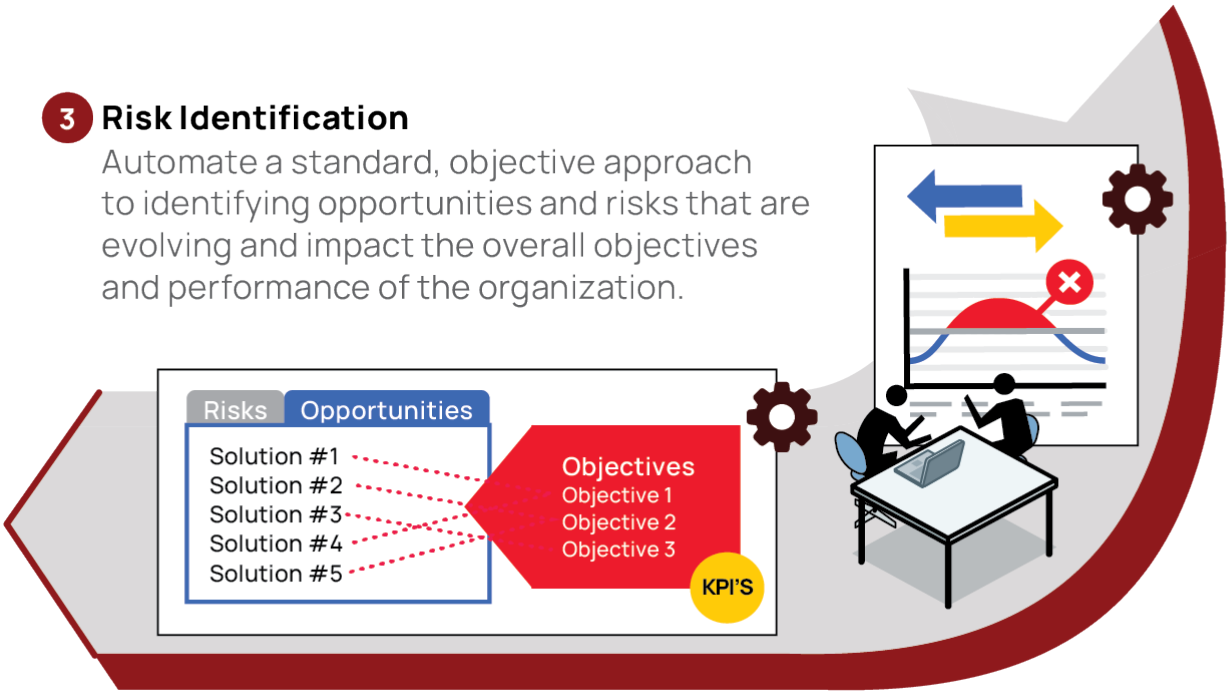
2. **Establish impact tolerances.** Next, it is critical to clearly define impact tolerances for objectives, processes, and services. Determine the level and type of risk the organization is willing to address, given the level and type of reward it pursues.

   - Impact tolerances define the acceptable level of impact or deviation from objectives that the organization is willing to tolerate. These tolerances should be aligned with the organization's risk appetite and strategic goals.
   - Define impact tolerances for objectives, processes, and services based on their criticality, importance, and sensitivity to risk.
   - When establishing impact tolerances, consider factors such as financial impact, reputational damage, regulatory compliance, and operational disruption.
   - Engage key stakeholders, including senior management and subject matter experts, in defining impact tolerances to ensure alignment with organizational priorities.



3. **Risk identification.** In this step, the organization takes a standard, objective approach to identifying evolving opportunities and risks that impact its overall objectives and performance.

   - Implement automated tools and systems to facilitate a standardized and objective approach to identifying risks and opportunities.
   - Utilize data analytics, machine learning algorithms, and other advanced techniques to identify emerging risks and trends that may impact the organization's objectives and performance.
   - Establish risk registers or databases to systematically capture and categorize identified risks, including their potential impact and likelihood of occurrence.
   - Encourage active participation from employees at all levels of the organization in identifying risks. They often have valuable insights into potential vulnerabilities and opportunities for improvement.



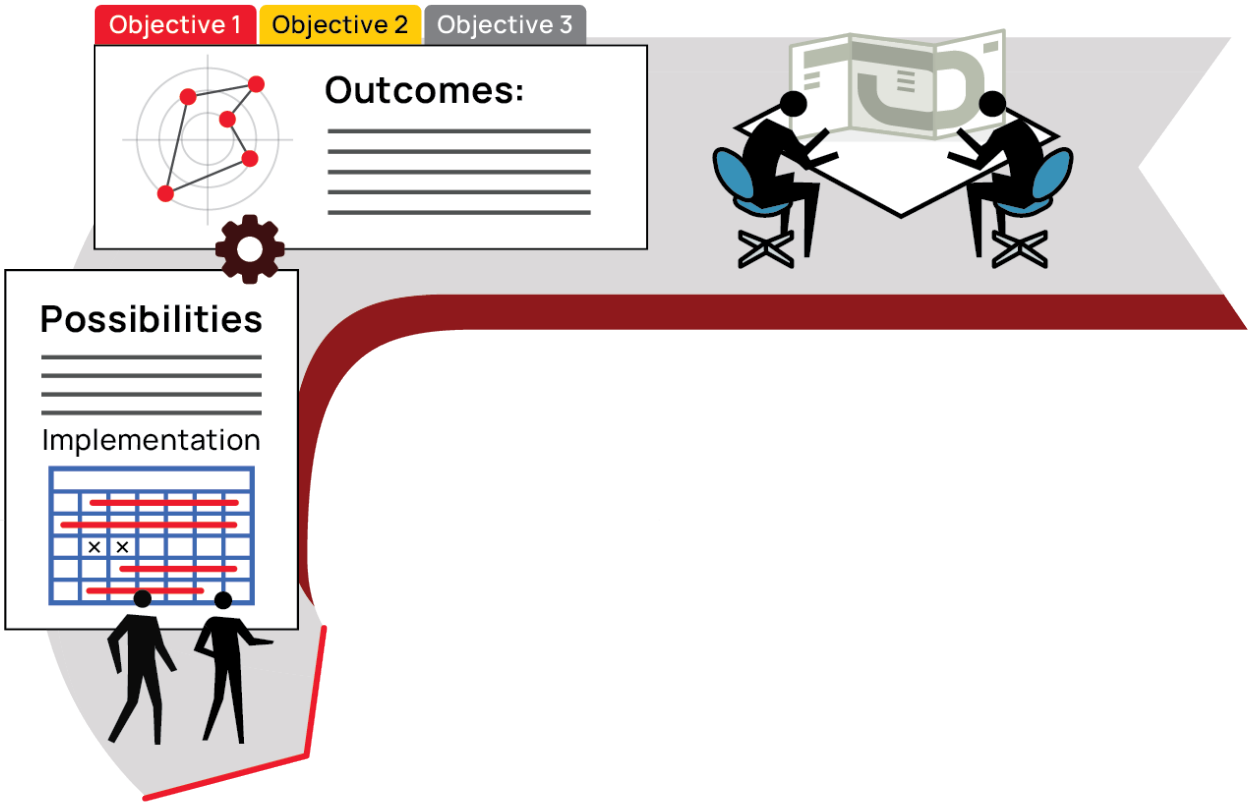
4. **Risk assessment.** Here, the organization identifies the possibilities of outcomes and their impact on achieving objectives. This includes a variety of risk analysis and assessment techniques (e.g., bow-tie risk assessments, scenario analysis, Monte Carlo).

   - Conduct comprehensive risk assessments to evaluate the potential consequences of identified risks on achieving objectives.

- Employ various risk analysis and assessment techniques, such as bow-tie risk assessments, scenario analysis, and monte carlo simulations, to quantify and prioritize risks.
- Assess each risk's likelihood and impact, taking into account the organization's risk tolerances and appetite.
- Consider the interdependencies between different risks and their cumulative impact on the organization's objectives and performance.

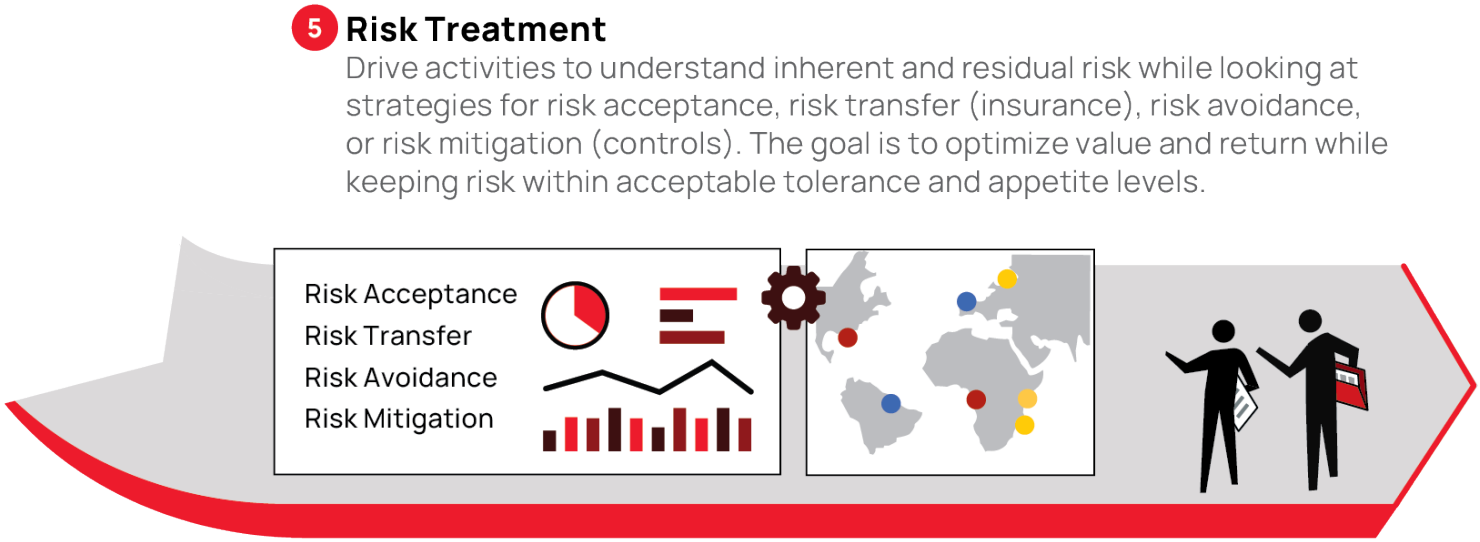
4 Risk Assessment

Identify the possibilities of outcomes possible impact on achievement of objectives. This includes a variety of risk analysis and assessment techniques (e.g., bow-tie risk assessments, scenario analysis, monte carlo).



5. **Risk treatment.** The assessment then drives activities to understand inherent and residual risk while looking at strategies for risk acceptance, risk transfer (insurance), risk avoidance, _or risk mitigation (controls). The goal is to optimize value and return while keeping risk within acceptable tolerance and appetite levels.

   - Evaluate the identified risks to determine appropriate risk treatment strategies.
   - Analyze both inherent and residual risks associated with each objective, process, or service.
   - Explore options for risk acceptance, risk transfer (e.g., insurance), risk avoidance, and risk mitigation through implementing controls or other measures.
   - Prioritize risk treatment actions based on their potential impact on achieving organizational objectives and the cost-effectiveness of mitigation measures.

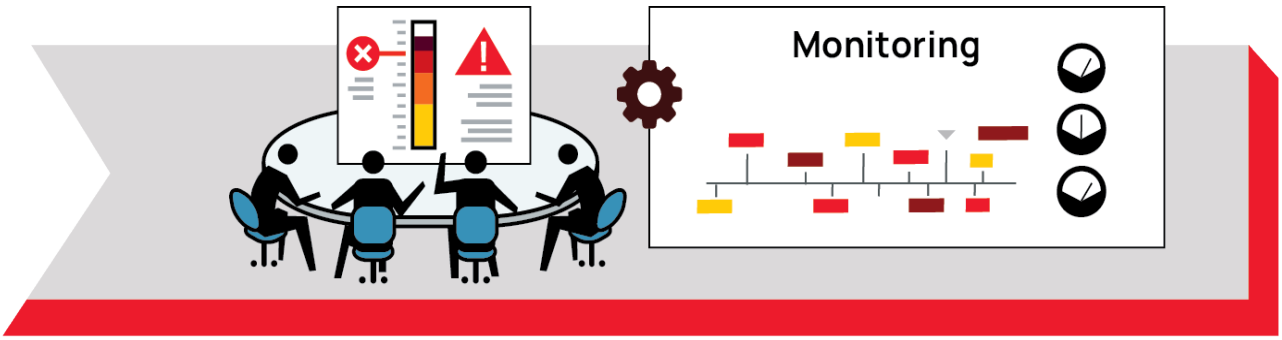


6. **Risk and resilience monitoring.** Then, the organization needs a range of processes to continuously monitor risks. These activities are typically done within the organization to monitor and assess risks on an ongoing basis.

   - Implement a range of processes and tools to monitor risks continuously throughout the organization.
   - Utilize key risk indicators (KRIs) and performance metrics to track changes in risk levels and trends over time.

6 Risk and Resilience Monitoring

Apply a range of processes to monitor risks continuously in the organization. These activities are the ones typically done within the organization to monitor and assess risks on an ongoing basis.



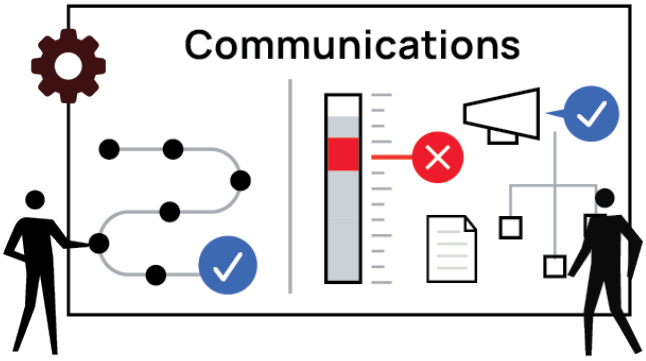
- Establish regular risk review meetings or forums where stakeholders can discuss and assess the effectiveness of risk mitigation measures.
- Leverage technology solutions such as risk management software and dashboards to provide real-time visibility into the organization's risk profile and resilience capabilities.

7. **Risk and resilience communications and attestations.** The organization needs to manage communication and interactions with risk owners throughout these processes. These are done periodically or when certain risk conditions are triggered.

- Establish ongoing processes for communication and interaction with risk owners and stakeholders.
- Develop clear communication channels and protocols for sharing risk-related information, updates, and recommendations.
- Conduct periodic risk attestation exercises where stakeholders formally acknowledge their understanding of risks and their responsibilities for managing them.
- Ensure that risk and resilience communications are timely, transparent, and aligned with organizational objectives and priorities.

7 Risk and Resilience Communications & Attestations

Run ongoing processes to manage communication and interactions with risk owners. These are done periodically, or when certain risk conditions are triggered.



Risk and Resilience Management Information & Technology Architecture

The risk and resilience management information architecture supports the process architecture and overall risk and resilience management strategy. With processes defined and structured, the organization can now define the information architecture needed to support them. The information architecture involves the structural design, labeling, use, flow, processing, and reporting of risk and resilience management information to support the necessary processes.

A successful risk and resilience management information architecture can connect information across risk management and business systems. This requires a robust and adaptable risk and resilience information architecture that can model the complexity of risk information, transactions, interactions, relationships, cause and effect, and the analysis of information, which can integrate and manage a range of business systems and external data.

The risk and resilience management technology architecture operationalizes the information and process architecture to support the overall risk and resilience management strategy. The right technology architecture enables the organization to manage risk effectively and facilitates the ability to document, communicate, report, and monitor a range of risk assessments, documents, tasks, responsibilities, and action plans.

Many organizations see risk and resilience management initiatives fail when they purchase technology before understanding their process, information architecture, and requirements. Risk and resilience management also fails when information is scattered, redundant, non-reliable, and managed as a system of parts that do not integrate and work collectively. Organizations have the following technology architecture choices before them:

- **Documents, spreadsheets, and email.** Manual spreadsheet and document-centric processes are prone to failure, as they bury the organization in mountains of data that are difficult to maintain, aggregate, and report on—consuming valuable resources. The organization ends up spending more time on data management and reconciling, as opposed to active risk monitoring.

- **Scattered point solutions.** Implementation of several point solutions that are deployed and purpose-built for particular risk and regulatory issues. The challenge here is that the organization maintains a wide array of solutions that do very similar things but for different purposes. This introduces a lot of redundancy in information gathering and communication that taxes the organization in managing risk holistically.

- **Risk and resilience management platform.** This is the current generation of GRC technology that provides for robust integration of risk and resilience management. This technology manages risk to bring it to a centrally connected hub for overall analysis and reporting. In this context, technology takes a balanced view of risk and resilience management that includes objectives and performance, as well as risk and control needs. These solutions allow an

organization to govern risk throughout its lifecycle and enable enterprise risk reporting and integration of risk throughout the enterprise.

There can and should be a central core technology platform for risk and resilience management that connects the fabric of risk processes, information, and other technologies across the organization. This platform is the hub of risk management and requires that it be able to integrate and connect with a variety of other businesses—specialized and focused risk systems, as well as external risk data sources.

The right risk and resilience management technology architecture choice for an organization often involves integrating several components into a core risk and resilience management platform solution, which can facilitate the integration and correlation of risk information, analytics, and reporting. Organizations suffer when they take a myopic view of risk management technology that fails to connect all the dots and provide context to business analytics, performance, objectives, and strategy in the real-time that a business operates in.

Risk and resilience management platforms help organizations identify, assess, and manage risks and opportunities while enhancing their resilience. These systems pinpoint specific causes and allow for historical review, future simulation, and analysis of how different events might impact the organization's operations or assets, considering how likely these events are to happen and whether they might occur one after the other or simultaneously.

Risk technology has evolved. GRC 20/20 has monitored this over the years, and we have seen progression that allows for greater user experience while providing connectivity and integration with other systems to consume and share data. Modern risk and resilience management platforms have advanced analytical capabilities and leverage artificial intelligence and cognitive computing with predictive analytics, machine learning, and natural language processing.

Some of the core capabilities organizations should consider in their risk and resilience management technology platform are:

- **Overall risk and resilience program management.** A comprehensive risk and resilience management platform should be the central hub for managing the organization's risk and resilience initiatives. It should provide functionalities for planning, executing, and monitoring the overall risk and resilience program. This includes defining program objectives, establishing governance structures, allocating resources, tracking progress, and reporting on key metrics and performance indicators. The platform should facilitate stakeholder collaboration and seamless communication and coordination across departments and functions.

- **Support for strategic, enterprise, and operational risk and resilience.** The platform should cater to the diverse risk management needs of the organization, spanning strategic, enterprise-wide, and operational levels. It should offer capabilities to assess and manage risks across all business areas, including

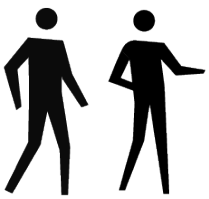
financial, operational, compliance, and reputational risks. This entails aligning risk management activities with strategic objectives, integrating risk management processes into day-to-day operations, and fostering a culture of risk awareness and accountability throughout the organization.

- **360° contextual awareness of risks to objectives.** A critical capability of the platform is to provide a holistic view of risks in relation to organizational objectives. It should enable stakeholders to understand the context and significance of risks by providing contextual information such as the impact on key objectives, dependencies, and interrelationships between risks. This 360-degree awareness helps prioritize risk management efforts, allocate resources effectively, and make informed decisions to mitigate risks and enhance resilience.

- **Risk identification, analysis, treatment, and monitoring.** The platform should support the entire risk management lifecycle, from identification and analysis to treatment and monitoring. This includes functionalities to identify and assess risks, understand their potential impact on objectives, establish impact tolerances and risk appetite, develop risk treatment plans, and monitor risk mitigation activities. Advanced analytical tools and techniques should be

Critical Capabilities

- Overall risk and resilience program management
- Support for strategic, enterprise, and operational risk and resilience
- 360° contextual awareness of risks to objectives
- Risk identification, analysis, treatment & monitoring
- Identify objectives, processes, services
- Understand & map risk relationships
- Establish impact tolerances and risk appetite
- Scenario & business impact analysis, risk forecasting, and planning
- Risk quantification, normalization & aggregation
- Allocate risk accountability
- Advanced risk reporting and trending
- Continuity & resilience plan management
- Corrective /Preventive Action Plans
- Crisis & Risk Event Management



integrated to facilitate risk analysis, scenario planning, and predictive modeling for proactive risk management.

- **Identify objectives, processes, and services.** The platform should facilitate identifying and documenting organizational objectives, processes, and services to provide a foundation for effective risk management. This involves capturing detailed information about the organization's strategic goals, business processes, and critical services, including interdependencies and relationships with key stakeholders.

- **Understand & map risk relationships.** Effective risk management requires a clear understanding of the relationships between risks, objectives, processes, and services. The platform should enable stakeholders to map these relationships visually and analyze the potential impact of risks on various aspects of the organization. This capability helps identify cascading or systemic risks, prioritize mitigation efforts, and optimize resource allocation for maximum risk reduction.

- **Establish impact tolerances and risk appetite.** The platform should support the establishment of impact tolerances and risk appetite to guide risk management decisions. It should provide tools and frameworks for defining acceptable levels of risk exposure and articulating the organization's willingness to take risks in pursuit of its objectives. This capability enables stakeholders to align risk management activities with strategic priorities and make informed trade-offs between risk and reward.

- **Scenario & business impact analysis, risk forecasting, and planning.** The platform should facilitate scenario analysis, business impact assessment, and risk forecasting to anticipate potential risks and plan appropriate response strategies. It should enable stakeholders to simulate different scenarios, assess the likelihood and severity of risk events, and evaluate the possible consequences on business operations and objectives. This capability supports proactive risk management and effectively prepares the organization for contingencies and uncertainties.

- **Risk quantification, normalization, and aggregation.** The platform should offer robust capabilities for quantifying, normalizing, and aggregating organizational risks. It should provide methodologies and algorithms for assigning numerical values to risks, standardizing risk metrics for comparability, and aggregating risks at various levels of granularity (e.g., strategic, operational, enterprise-wide). This capability facilitates risk prioritization, resource allocation, and decision-making based on quantitative risk analysis.

- **Allocate risk accountability.** The platform should enable the allocation of risk accountability by defining roles, responsibilities, and ownership for managing specific risks. It should provide mechanisms for assigning accountability to individuals or teams, tracking their progress in addressing assigned risks, and ensuring accountability throughout the risk management process. This capability

fosters a culture of ownership and accountability for risk management across the organization.

- **Advanced risk reporting and trending.** The platform should offer advanced reporting and analytics capabilities to communicate risk-related information effectively to stakeholders. It should provide customizable dashboards, reports, and visualizations to present key risk metrics, trends, and insights in a clear and actionable manner. Additionally, the platform should support trend analysis, benchmarking, and predictive analytics to identify emerging risks and monitor changes in the risk landscape over time.

- **Continuity and resilience plan management.** The platform should facilitate developing, implementing, and managing continuity and resilience plans to ensure business continuity in the face of disruptions. It should support creating comprehensive plans for incident response, crisis management, business continuity, and disaster recovery, including predefined workflows, communication protocols, and escalation procedures. This capability helps the organization minimize the impact of disruptions and maintain operational resilience.

- **Corrective/Preventive Action Plans.** The platform should enable the creation and management of corrective and preventive action plans to address identified risks and vulnerabilities. It should provide tools for documenting corrective actions, assigning responsibilities, setting timelines, and tracking progress toward implementation. This capability ensures that risks are addressed promptly and systematically, reducing the likelihood of recurrence and enhancing the organization's resilience.

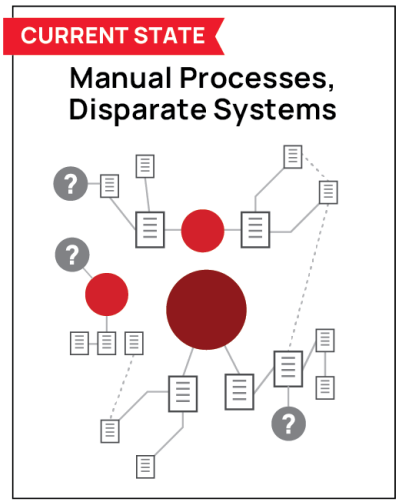
- **Crisis and Risk Event Management.** The platform should support effective crisis and risk event management by providing tools and resources to respond swiftly and decisively to unexpected events. It should enable stakeholders to activate predefined response plans, coordinate response efforts, communicate with internal and external stakeholders, and track the resolution of incidents in real-time. This capability helps minimize the impact of crises, restore normal operations, and mitigate reputational damage to the organization.

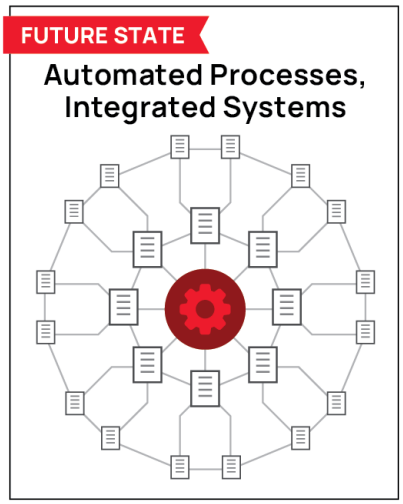
Building a Business Case for Risk & Resilience Management

The performance and usability of the new generation of connected and integrated risk and resilience management platforms, in the context of GRC technology, return value to the organization through efficiency, effectiveness, resilience, and agility—providing the overall solid performance of the solution and agility and rapid implementation timeframes through a low-code configurable solution.

Building a comprehensive business case to improve an organization's risk and resilience program involves a detailed current state analysis of where the organization is today in its strategy, processes, and technology for risk and resilience management. For many, this is a maze of point solutions and thousands, if not tens of thousands, of documents, spreadsheets, and emails scattered across silos of risk management that do not talk to

each other. Others may find they have a mature and established program that needs minor adjustments.





After the current state analysis is complete, the organization defines the future state. What is the ideal design of risk and resilience management to provide value to the business in pursuit of its objectives? This is the future state. It is then necessary to build a roadmap and project plan for moving from the current state to the future state.

With a clearly defined future state for risk and resilience management strategy, governance, process, information, and technology, the organization can quantify the value of moving to that state across the following four areas.

- **Efficiency.** Efficiency is crucial for organizations striving to optimize resources and maximize productivity. Implementing the right risk and resilience management solution can yield substantial efficiency gains by streamlining processes and reducing unnecessary costs. By automating manual tasks such as data entry, reporting, and compliance tracking, the solution frees up valuable human capital, allowing employees to focus on higher-value activities. This saves time, reduces the risk of errors, and ensures data accuracy. Furthermore, centralizing risk-related information in a single, integrated platform eliminates redundancy and duplication, leading to more efficient resource allocation and decision-making. Ultimately, the organization can achieve cost savings in terms of both human capital and financial capital, enhancing overall operational efficiency.

- **Effectiveness.** Effectiveness in risk and resilience management is essential for effectively mitigating potential unwanted risk exposure and seizing opportunities. The right solution empowers the organization to identify, assess, and mitigate risks comprehensively, reducing the likelihood of issues slipping through the cracks. With enhanced visibility and real-time monitoring capabilities, stakeholders can proactively manage risks, leading to greater management and accountability. By providing actionable insights and customizable reporting tools, the solution enables stakeholders to make informed decisions and take timely actions to address emerging risks. This minimizes the impact of risk events and enhances the organization's ability to achieve its strategic objectives and deliver value to stakeholders.

- **Resilience.** Organizational resilience is critical for surviving and thriving in today's dynamic business environment. A robust risk and resilience management solution is pivotal in building resilience by enabling the organization to anticipate, prepare for, and respond to disruptions effectively. By identifying and containing risk issues early on, the solution minimizes the organization's exposure to potential threats, safeguarding its operations and reputation. Through scenario analysis, business impact assessments, and continuity planning, the solution

Efficiency
The right risk and resilience management solution will save time and money (human capital and financial capital costs).

Effectiveness
The right risk and resilience management solution will see fewer things slipping through the cracks and greater management and accountability of risk.

Resilience
The right risk and resilience management solution will enable the organization to identify and contain risk issues, minimizing risk exposure to the organization.

Agility
The right risk and resilience management solutions will enable the organization to forecast risk developing on the horizon and prepare the organization for the best path forward.

helps the organization develop proactive strategies to mitigate the impact of adverse events and ensure business continuity. This enhances the organization's ability to adapt to change, recover from disruptions, and maintain long-term sustainability.

- **Agility.** Agility is essential for organizations to navigate uncertainty and seize opportunities in a rapidly evolving business landscape. The right risk and resilience management solutions enable the organization to swiftly anticipate and respond to emerging risks, enhancing agility. By leveraging advanced analytics and predictive modeling, the solution forecasts risk developments on the horizon, allowing stakeholders to prepare and adapt their strategies accordingly. Through scenario planning and stress testing, the solution helps the organization assess its readiness to withstand various scenarios and adjust its plans as needed. This proactive approach to risk management enhances the organization's agility, enabling it to stay ahead of the curve, capitalize on market opportunities, and maintain a competitive edge.

Investing in the right risk and resilience management strategy and solution delivers tangible benefits across efficiency, effectiveness, resilience, and agility. By optimizing resource allocation, enhancing risk management practices, building organizational resilience, and fostering agility, the organization can mitigate risks, seize opportunities, and drive sustainable growth in the long run.

GRC 20/20's Final Perspective

Growing in Risk & Resilience Management Maturity

Successful risk and resilience management requires the organization to provide an integrated process, information, and technology architecture. This helps identify, analyze, manage, and monitor risk and capture changes in the organization's risk profile from internal and external events. Mature risk and resilience management is a seamless part of governance and operations. It requires the organization to take a top-down view of risk, led by the executives and the board, and makeup part of the fabric of the business, not

an unattached layer of oversight. It also involves bottom-up participation where business functions at all levels identify and monitor uncertainty and the impact of risk.

Risk and resilience management in business is non-linear. It is not a simple equation of 1 + 1 = 2. It is a mesh of exponential, sometimes chaotic, relationship and impact in which 1 + 1 = 3, 30, or 300. What seems like a minor disruption or exposure may have a massive or no effect. In a linear system, the effect is proportional to the cause; risks are exponential in the non-linear business world. Business is chaos theory realized. The small flutter of risk exposure can bring down the organization. If we fail to see the interconnections of risk in the non-linear business world, the result is often exponential to unpredictable.

Mature risk and resilience management enables the organization to understand objectives and performance in the context of risk. It can weigh multiple inputs from both internal and external contexts, use various methods to analyze risk, and provide qualitative and quantitative modeling.

Organizations striving to increase risk and resilience management maturity in their organization become more:

- **Aware.** They want to have a finger on the pulse of the business and watch for change in the internal and external environments that introduce risk. The key is to turn data into information that can be analyzed and shared in every relevant direction.

- **Aligned.** They must align performance and risk management to support and inform business objectives. This requires continuously aligning the objectives and operations of the integrated risk capability to the objectives and operations of the entity and giving strategic consideration to information from the risk management capability to affect appropriate change.

- **Responsive.** Organizations cannot react to something they do not sense. Mature risk and resilience management focuses on gaining greater awareness and understanding of information that drives decisions and actions, improves transparency, and quickly cuts through the morass of data to what an organization needs to know to make the right decisions.

- **Agile.** Stakeholders desire the organization to be more than fast; they require it to be nimble. Being fast isn't helpful if the organization is headed in the wrong direction. Mature risk and resilience management enables decisions and actions that are quick, coordinated, and well thought out. Agility allows an entity to use risk to its advantage, grasp strategic opportunities, and be confident in its ability to stay on course.

- **Resilient.** The best-laid plans of mice and men fail. Organizations need to be able to bounce back quickly from changes in context and risks with limited business impact. They desire sufficient tolerances to allow for some missteps and the confidence necessary to adapt and respond rapidly to opportunities.

- **Efficient.** They want to build business muscle and trim fat to rid expense from unnecessary duplication, redundancy, and misallocation of resources and to make the organization leaner overall with enhanced capability and related decisions about the application of resources.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com