April 2022

Risk & Resiliency Management by Design

An Integrated Approach to Risk & Resilience Management

STRATEGY***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

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 & Resiliency Management by Design

An Integrated Approach to Risk & Resilience Management

360° Visibility into Risk & Resilience

Dynamic, Disrupted & Distributed Business is Difficult to Control

Organizations take risks all the time but fail to monitor and manage these risks effectively in an environment that demands agility. 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 is a result of a poorly defined risk culture. It 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.

The complexity of business – combined with the intricacy and interconnectedness of risk and objectives – necessitates that the organization implements a strategic and integrated approach to risk and resilience management across the organization. This includes a top-down enterprise approach aligned with objectives as well as a bottom-up operational approach focused on risk and resilience in the depths of the organization.

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 encumbers organizations of all sizes. Keeping changes to business strategy, operations, and processes in sync is a significant challenge. Organizations need to see the intricate relationships and impacts of objectives, risks, processes, and controls.

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

- **Interconnected risk.** Organizations face an interconnected risk environment; risk, and resilience cannot be managed in isolation. What started with a health and safety risk became a global pandemic and had downstream risk impacts on information security, bribery and corruption, fraud, business and operational resilience, human rights, and other risk areas.

- **Objectives became dynamic.** As the pandemic unfolded, it had a specific impact on business objectives. Adapting to the crisis, businesses had to modify their

strategies, departments, processes, and project objectives in reaction to changes in risk exposure.

- **Disruption.** Business is easily disrupted from international to local events. Organizations had to respond to disruption from the pandemic, political protests and unrest, economic uncertainty, change in business models and a work from home environment, human rights and discrimination protests, environmental disasters (particularly wildfires), and information security breaches (e.g., SolarWinds, Colonial Pipeline).

- **Dependency on others.** No organization is an island. The past two years have shown us that disruption and the interconnectedness of risk and resilience impacts more than traditional employees and brick-and-mortar business, but also the range of third-party relationships in the extended enterprise that the organization depends upon.

- **Dynamic and agile business.** Businesses had to react quickly to stay in business. This required agility in changing employees, reduced staff with more responsibilities, and shifting to work from home environments. All this introduced new risks, as well as a demand for engaging employees and maintaining a strong corporate culture amid global uncertainty.

- **Values were defined and tested.** Organizations had to react to what their core values were and how they practiced those values. From treating employees and customers fairly during a crisis, to how they address human rights.

This has taught organizations that to be resilient requires a 360° view of objectives, risk, processes, and services within the organization and the extended enterprise.

Understanding the Interrelationship of Risk and its Impact on Operations

Risk management is often misunderstood, misapplied, and misinterpreted as a result of scattered and uncoordinated approaches that get in the way of sharing data. Risk is pervasive; there are a variety of departments that manage risk with varying approaches, models, needs, and views on what risk is and how it should be measured and managed. These challenges come at department and process levels and continue to build as organizations develop risk and resilience management strategies that span these departments.

For some organizations, risk management is only an expanded view of routine financial controls, resulting in nothing more than a deeper look into internal controls with some heat maps thrown in, and does not truly provide an enterprise view of risk aligned with strategy and objectives. Completing a risk assessment process and ticking the box has got in the way of true risk analysis and understanding.

Risk management is about the risk of not achieving objectives, therefore making the ability to link and measure risk to strategic objectives critical as well as the resiliency of the organization in achieving those objectives in a chaotic world; as is monitoring

performance against those objectives. The outcome of this is improved decision-making, better return on investment across the business, improved profitability, and a better customer experience.

Risk management silos — where distributed business units and processes maintain their own data, spreadsheets, analytics, modeling, frameworks, and assumptions — pose a major challenge to achieving this. 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 and not the aggregate picture, unable to 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. This is because it intersects, compounds, and interrelates to create a larger risk exposure than each silo is independently aware of. A siloed approach fails to deliver insight and context and renders it nearly impossible to make a connection between risk management and decision-making, business strategy, objectives, and performance. Risk accountability is frequently distributed across different board level owners. Today it is critical that these roles are all working off the same data and that this risk data is clean, reliable, and timely.

It can be bewildering to make sense of risk management and its varying factions across strategic, financial, credit, market, conduct, operational, continuity, project, legal, regulatory, third-party, strategic, insurance, and hazard risks. It makes enterprise and operational risk management a challenge if a risk management strategy forces everyone into one flat view of risk, confirming to have significant issues in risk normalization and aggregation as they roll-up risk into enterprise risk reporting. This is exponentially compounded when risk velocity is considered: when risk materializes into an event it moves very quickly. Are organizations agile enough to react?

Keeping risk, complexity, and change in sync is a significant challenge for boards, executives, and management professionals throughout all levels of the organization. This challenge is even greater when risk management is buried in the depths of departments and approached from a compliance or audit angle, and not as an integrated discipline of decision-making that has a symbiotic relationship on performance and strategy. This further is compounded when business continuity programs are completely disconnected and not part of risk management. Organizations need to understand how to monitor risk-taking, measure that the associated risks being taken are the right risks, and review whether the risks are managed effectively to ensure resilience of the organization.

Risk and resiliency management in the modern organization is challenging because the organization is:

- **Distributed.** 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 which define the organization. Complexity grows as these interconnected relationships, processes, and systems nest themselves in intricacy.

- **Dynamic.** Organizations are in a constant state of 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 span regulatory, geopolitical, market, credit, and operational risks. Managing risk and business change on numerous fronts buries the organization when managed in silos.

- **Disrupted.** Organizations face an complex and chaotic global 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.

- **Accountable.** There is growing awareness among executives and directors that risk management needs to be taken seriously. It is part of their fiduciary obligations to oversee risk management as an integrated part of business strategy and execution.

Resilience is not business continuity 2.0. It is much more than that. Risk and resilience management is an integrated effort that requires collaboration, processes, and information/technology shared between operational risk management, business continuity management, and even third-party risk management.

Operational Resilience Definitions

Operational resilience is a growing regulatory concern in the financial services industry. This is how the financial regulators define operational resilience:

- **UK FCA:** We define 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.
- **EU DORA:** 'digital operational resilience' means the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality.
- **US OCC:** Operational resilience is the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.
- **Basel Committee on Banking Supervision:** 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.

Providing 360° Contextual Awareness of Risk and Resilience

The physicist, Fritjof Capra, made an insightful observation on living organisms and ecosystems that also 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."
Fritjof Capra

Capra's point is that biological ecosystems are complex, interconnected, and require a holistic understanding of the intricacy in interrelationships as an integrated whole, rather than a dissociated collection of parts. Change in one segment of an ecosystem has cascading effects and impacts to the entire ecosystem. Consider the interconnectedness of a cycle of risk in the context of a drought and a forest fire. A drought increases the risk of a forest fire. If a fire should start this further contaminates the water as a byproduct of the fire. As the forest regrows it further reduces the water supply to sustain this growth which could cause more drought conditions.

Organizations need complete 360° situational awareness and visibility into 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, as well as how it impacts their strategy and objectives. The organization needs visibility into objective and risk relationships across processes. Complexity of business and intricacy, as well as the interconnectedness of risk data, requires that the organization implement an enterprise view of risk and resilience monitoring, automation, and enforcement.

The ecosystem of business objectives, uncertainty/risk, and integrity is complex, interconnected, and requires a holistic contextual awareness of the organization – rather than a dissociated collection of processes and departments. This interconnectedness of business is driving demand for 360° contextual awareness in the organization's risk and resilience processes to reliably achieve objectives, address uncertainty, and act with integrity. Organizations need to see the intricate intersection of objectives, risks, and boundaries across the business. The interconnectedness of objectives, strategy, risks, and continuity require 360° contextual awareness of risk and resiliency.

Firms globally and across industries are focusing on integrating their risk management resilience (historically business continuity/disaster recovery) programs. This is becoming a key regulatory requirement in some industries. Delivering this requires a holistic view into the objectives and processes of the organization in the context of uncertainty and risk and the symbiotic interaction of risk management and business continuity.

The Risk & Resilience Central Nervous System

Organizations need to develop a risk management capability aligned with strategy, performance, and objectives that operate as a risk central nervous system. Consider the following from Steve Balmer:

> *"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."*
>
> Steve Balmer, former CEO Microsoft

A nervous system connects with other major systems of the body, and provides among others analytical capability, strategic thinking, and quick response to the environment.

In the same context, organizations need a command and control hub that provides the analytical capability to measure and monitor a connected view of risk across:

- Strategy
- Operations
- Continuity & Resilience
- Compliance & Regulatory
- Reputational
- Conduct
- Market
- Insurance
- Credit
- Liquidity

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. This is an important part of developing a risk analysis framework. Mature risk management is built on a risk management process, information, and technology architecture that can show the relationship between objectives, risks, controls, loss, and events. The demand is for predictive analytics to extract from this mass amount of data what exactly will help to prevent future significant losses, events, as well as incidents, and further help strategic business objectives succeed.

This means enabling a federated and connected view of risk that leverages artificial intelligence, machine learning, and robotic process automation to make the risk management process more efficient, effective, and agile. This in turn enables organizations to spend more time focusing on the analysis of risk 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:

- How does the organization know it is taking and managing 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 make 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 individual objective or process, and how it interrelates with other risks to aggregate into an enterprise perspective of risk?
- Can the organization accurately gauge the impact risk has on strategy, performance, project, process, department, division, and enterprise levels?
- Does the organization have the information it needs to quickly respond to and avoid risk exposure, and also to seize risk-based opportunities?
- Does the organization monitor key risk indicators across critical projects and processes?
- Is the organization optimally measuring and modeling risk?

Gathering multiple perspectives on risk is critical for producing effective relational diagrams, decision trees, heat maps, and scenarios. This risk intelligence comes from:

- **The external perspective.** Monitoring the external environment for geopolitical, environmental, competitive, economic, regulatory, and other risk intelligence sources.

- **The internal perspective.** Evaluating the internal environment of objectives, projects, risks, controls, audits, loss, performance and risk indicators, and other internal data points.

The Bottom Line: Successful risk and resilience management requires the organization to provide an integrated strategy, process, information, and technology architecture. The goal is comprehensive straightforward insight into risk and resilience management to identify, analyze, manage, and monitor risk in the context of 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. Organizations need to clearly understand the breadth and depth of their integrated risk and resilience management strategy and process requirements, and from there select the right information and technology architecture that is agile and flexible to meet the range of risk management needs for today, and into tomorrow.

Risk & Resilience Management by Design

An Integrated Approach to Risk & Resilience Management

The primary directive of a mature risk and resilience management program is to deliver effectiveness, efficiency, and agility to the business. This is in the context of managing the breadth of risks of organizational performance, objectives, strategy, 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 better manage risk:

- **Anarchy – ad hoc department silos.** This is when the organization has departments doing different yet similar things with little to no collaboration between them. 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 is not thinking 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 then the natural reaction is the complete opposite: centralize everything and get everyone to work from one perspective. However, this has its issues as well. Organizations become susceptible to one department being in charge of managing risk, without perhaps fully understanding the breadth and scope of all of the necessary risk management priorities. The needs of one area may also

come to shadow the needs of others. From a technology point of view, it may force many parts of the organization into managing 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 will 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 governance model and architecture that the various groups across risk management participate in. A federated approach increases the ability to connect, understand, analyze, and monitor connectedness and underlying patterns of performance, risk, and control across risk relationships. Mainly it allows different business functions to be focused on their areas while reporting into a common 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 risk and resilience management strategy. The strategy connects key business functions with a common risk governance framework and policy. The strategic plan is the foundation that enables risk transparency, discipline, and control of the ecosystem of risk 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 gets 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, 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 key 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 key 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 reporting on risk and resilience management.

- **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, associated responsibilities, approvals, assessments, evaluation, audits, and reporting. The policy should require that an inventory of all risks be maintained with appropriate categorizations, approvals, and identification of risks.

Risk and Resilience Management Architecture

The risk and resiliency 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, 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

It is critical that these architectural areas be initially defined in this order. It is the risk and resilience management processes that determine the types of risk information needed, gathered, used, and reported. It is the information architecture combined with the process architecture that 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 a technology for risk management instead of finding the technology that best fits their risk process and information needs.

Risk and Resilience Management Process Architecture

Risk and resilience management processes are a part and subset of overall business processes. Processes 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, as well as 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:

- **Objective, process & service identification.** The first step is to define, map, and model the organization's objectives, processes, and services. Objectives can be defined at different levels such as entity, division, department, process, service, project, or even asset level objectives. Risk is formally the effect of uncertainty on objectives. This necessitates that the organization also fully define, map, and model its business processes and services to understand risk and resiliency in the context of the organization's operations.

- **Establish impact tolerances.** Next, the organization needs to clearly define impact tolerances for objectives, processes, and services. This includes a clear understanding of what some call risk appetite, but is more than that.

- **Risk identification.** This is the collection of processes aimed at automating a standard, objective approach for identifying risk. Understand your surroundings. It is about the internal business context, the external environment that the business operates in, and your strategy as to where the business is heading. On an ongoing basis, and separate from the monitoring of individual risks, is the ongoing process of monitoring risk in the context of external environments as well as the internal organization's environment. The purpose is to identify opportunities and risks that are evolving and impact the overall objectives and performance of the organization. A variety of regulatory, environmental, economic, geopolitical, and internal business factors can affect the success or failure of any organization. This includes the potential for natural disasters, disruptions, commodity availability and pricing, industry developments, and geopolitical risks. This also involves monitoring relevant legal and regulatory environments in corresponding jurisdictions to identify changes that could impact the business and its objectives.

- **Risk assessment.** Once an organization identifies risks that can impact the business, it then can identify what can happen to help or hinder your objectives. An organization wants to identify the possibilities of outcomes, all the way to what can impact it from achieving its objectives. This should go beyond heat maps to include a variety of risk analysis and assessment techniques (e.g., bow-tie risk assessments, scenario analysis, Bayesian modeling). There are so many variables that can hinder the organization from achieving objectives. Some of these can be fairly evident and common sense, some can be very abstract,

remote, and down in the weeds of the organization. This requires tabletop exercises as well as risk scenario modeling and analysis to explore intuitively complex relationships of risks to other risks and objectives.

- **Risk treatment.** After the range of potential possibilities is understood, the organization needs to decide what to do. What is going to be the best route for the organization to achieve its objectives while minimizing loss and potential harm. This gets into risk measurement activities of understanding inherent and residual risk, while looking at strategies of risk acceptance, risk transfer (insurance), risk avoidance, or risk mitigation (controls). The goal is to optimize value and return while keeping risk within acceptable levels of tolerance and appetite. This also involves testing of scenarios and controls.

- **Risk and resilience monitoring.** This stage includes the array of processes to continuously monitor risks in the organization. These activities are the ones typically done within the organization to monitor and assess risks on an ongoing basis.

- **Risk and resilience communications & attestations.** Ongoing processes to manage the communication and interactions with risk owners throughout the risk and resilience management lifecycle. These are done on a periodic basis, or when certain risk conditions are triggered.

Effective risk and resilience management processes deliver:

- **Holistic awareness of risk.** There is a defined risk taxonomy across the enterprise that structures and catalogs risk in the context of business and assigns accountability. A consistent process identifies objectives, processes, services, risks, and impact tolerances and 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 and policy.** Risk policy must be communicated, monitored, and enforced across the organization 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 and are continuously mapped to organization performance and objectives. Technology monitors key risk indicators (KRIs) to ensure 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 — it is 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 of 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 management of risk 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 at their disposal. 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 reporting that is relevant to the business. The risk information adheres to information quality, integrity, relevance, and timeliness.

Risk and Resilience Management Information & Technology Architecture

Risk and resilience management fails when information is scattered, redundant, non-reliable, and managed as a system of parts that do not integrate and work as a collective whole. 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 risk and resilience management processes. 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 will be able to 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, relationship, 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 effectively manage risk, and facilitate the ability to document, communicate, report, and monitor a range of risk assessments, documents, tasks, responsibilities, and action plans.

There can and should be a central core technology platform for risk and resilience management that connects the fabric of the risk processes, information, and other technologies together across the organization. But this 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.

Many organizations see risk and resilience management initiatives fail when they purchase technology before understanding their process, and information architecture and requirements. 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 is difficult to maintain, aggregate, and report on - consuming valuable resources. The organization ends up spending more time in data management and reconciling, as opposed to active risk monitoring.

- **Point solutions.** Implementation of a number of point solutions that are deployed and purpose-built for very specific risk and regulatory issues. The challenge here is that the organization ends up maintaining 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.

- **Centralized risk management, GRC platforms.** These are solutions built specifically for risk management, and often have the broadest array of built-in (versus built-out) features to support the breadth of risk management processes. However, many of these systems were designed for specific risk purposes, and do not manage the breadth of risks well. There has also been issues of limitations in risk normalization and aggregation, as well as pushing many parts of the organization into a single view of risk that requires everyone to manage risk in one way.

- **Integrated risk and resilience management in a GRC 4.0/5.0 platform.** This is the current generation of GRC technology that provides for strong integration of both risk and resiliency management. This technology manages risk to bring it to a centrally connected hub for overall analysis and reporting. It is in this context that technology takes a balanced view of risk and resilience management that includes 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.

The right risk and resilience management technology architecture choice for an organization often involves the integration of 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 technology has evolved. GRC 20/20 has monitored this over the years, as we have seen progression that brings GRC related technologies into fourth-generation (Agile GRC) and now fifth-generation (Cognitive GRC) solutions. These solutions allow for greater user experience while providing connectivity and integration with other systems to consume and share data between systems. They have advanced analytical capabilities, and leverage artificial intelligence and cognitive computing with predictive analytics, machine learning, and natural language processing.

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

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

- **Integration.** Risk and resilience management is not a single, isolated competency or technology within a company. It needs to integrate well with other technologies and competencies that already exist in the organization - so the ability to pull and push data through integration is critical.

- **Content, workflow, and task management.** Content should be able to be tagged so it can be properly routed to the right subject matter expert to establish workflow and tasks for review and analysis. Standardized formats enable organizations to measure business impact, risk, and compliance.

- **360° contextual awareness.** The organization should have a complete view of what is happening with risk in the context of performance and compliance. Contextual awareness requires that risk management have a central nervous system to capture signals found in processes, data, and transactions. It also needs to capture changing risks and regulations for interpretation, analysis, and holistic awareness of risk in the context of risk and performance.

- **Support for multiple risk frameworks.** The risk management technology architecture should allow the organization to harmonize risk management across the enterprise. The business can use different risk management frameworks in various parts of the organization and still integrate risk data and reporting with an enterprise perspective.

- **Define and map objectives, processes, impact tolerances and controls to risk.** Controls are used to mitigate and monitor risk. Every control in the environment maps to the risks addressed, using an integrated risk and control framework. Risk technology should allow for the complete integration and reporting on objectives and controls in the context of their relationship to risk across the enterprise.

- **Establish and communicate risk policy.** Risk technology should allow the organization to develop, approve, and communicate policies to address risk. This establishes expectations and a culture around risk, including risk capacity, tolerance, appetite, accountability, and controls.

- **Manage loss and incidents.** Loss represents the materialization of risk and must be documented and fed into risk models. Risk technology enables the management of incidents and records loss as an integrated component of a risk management process.

- **Allocate risk accountability.** Risk management requires that someone is responsible for risk, and the right risk technology tracks ownership and steps taken to maintain compliance through a risk taxonomy, enforcing accountability through task management, workflow, and escalation. Through reporting and metrics, owners see risk from different perspectives and understand what they are responsible for.

- **Advanced risk reporting and trending.** Risk technology manages and monitors risk at the enterprise level and within individual departments. This permits detailed reporting, dashboards, trending, and analytics that scale to the needs of the department or enterprise. Organizations can establish and monitor risk metrics through KRIs and map them to objectives and processes. Reporting is customizable and scalable to the context and level of detail appropriate to the audience — whether it be process owners, managers, executives, or board members.

- **Risk analytics and modeling.** Mature risk technology should support a breadth of risk analytics and modeling to meet the diverse needs of groups across the business. The solution can track and model spending to treat risk in the context of exposure.

- **Understand the interrelationship of risk.** Risk technology provides for identification and categorization of risk into hierarchical structures to effectively manage and assign accountability. However, individual risks can also relate to risk outside of a hierarchical model. The risk information architecture allows for the categorization of risk, mapping, and the relationship of risk that does not always fit into neat hierarchies.

GRC 20/20's Final Perspective

Growing in Risk & Resilience Management Maturity

To maintain the integrity of the organization and execute on strategy, the organization has to be able to see the individual risk (the tree), as well as the interconnectedness of risk (the forest). Many organizations are asking for this to go even deeper, as they need to see the leaf and branch as it connects to the tree, and how it is part of the forest.

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, and a sometimes chaotic, relationship and impact in which 1 + 1 = 3, 30, or 300. What seems like a small disruption or exposure may have a massive effect or no effect at all. In a linear system, effect is proportional with cause, in the non-linear world of business, risks are exponential. 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 on the non-linear world of business, the result is often exponential to unpredictable.

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

Successful risk and resilience management requires the organization to provide an integrated process, information, and technology architecture. This helps to identify, analyze, manage, and monitor risk, and capture changes in the organization's risk profile from internal and external events as they occur. 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 make up part of the fabric of the business, not an unattached layer of oversight. It also involves a bottom-up participation where business functions at all levels identify and monitor uncertainty and the impact of risk.

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. Key to this is the ability to turn data into information that can be, and is, analyzed and shareable in every relevant direction.

- **Aligned.** They need to align performance and risk management to support and inform business objectives. This requires continuously aligning objectives and operations of the integrated risk capability to the objectives and operations of the entity, and to give 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 is focused on gaining greater awareness and understanding of information that drives decisions and actions, improves transparency, but also 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 to have sufficient tolerances to allow for some missteps and have the confidence necessary to rapidly adapt and respond to opportunities.

- **Efficient.** They want to build business muscle and trim fat to rid expense from unnecessary duplication, redundancy, and misallocation of resources; 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