February 2022

Risk & Resiliency Management Maturity Model

A New Paradigm in Risk, Resiliency & Continuity Integration

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 Maturity Model

A New Paradigm in Risk, Resiliency & Continuity Integration

360° Visibility into Risk & Resilience

Dynamic, Disrupted & Distributed Business is Difficult to Control

The complexity of business – combined with the intricacy and interconnectedness of risk and objectives – necessitates that the organization implements a strategic approach to business and operational risk and resilience.

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 for boards and executives, as well as management professionals throughout all levels of the business. The interconnectedness of objectives, risks, resilience, and integrity require 360° contextual awareness of risk and resiliency. Organizations need to see the intricate relationships and impacts of objectives, risks, processes, and controls. It requires holistic visibility and intelligence into risk and resiliency.

What Have We Learned from 2020 and 2021?

2020 and 2021 brought organizations 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 and 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.

The past two years have taught organizations that to be resilient requires a 360° view of objectives, risk, processes, and services within the organization and the extended enterprise.

The Risk Challenge to Boards, Executives, and Management

Organizations take risk all the time but fail to monitor and manage this risk 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. It results in inevitable failure of risk management, providing case studies for future generations on how poor risk and resiliency management leads to the demise of organizations - even those with strong brands.

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 are 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.

Integrated Risk & Resilience is the Way Forward

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. Change in one area has cascading effects that impacts the entire ecosystem.

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.

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.

Business or Operational Resilience?

Business resilience is broader than operational resilience but also includes operational resilience. Consider the following . . .

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.

- *Business resilience* is focused on the overall resilience of the organization, which includes strategy, liquidity/cash, diversity/hedging, culture/integrity, and operational resilience.

- *Operational resilience* is a component of business resilience focused on business processes, services, people, systems, and relationships.

Operational resilience is not business continuity 2.0. It is much more than that. Operational resilience 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.

Providing 360° Integrated Awareness of Risk and Resilience

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. 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 Bottom Line: Successful risk and resilience management requires the organization to provide an integrated strategy, process, information, and technology architecture. The goal is comprehensive straight forward insight into risk and resilience management to identify, analyze, manage, and monitor risk in 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. As a result, organizations are measuring their current state and planning toward a future state of increased risk and resilience maturity in the organization.

Risk & Resiliency Management Maturity Model

A New Paradigm in Risk, Resiliency & Continuity Integration

Lacking an integrated view of risk and resilience results in business processes, services, employees, and systems that behave like leaves blowing in the wind. Organizations need to develop, nurture, and mature a risk and resilience management capability aligned with strategy, performance, and objectives that operate as a risk and resilience 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 risk and resilience nervous system connect with other major systems of the body, and provides among others analytical capability, strategic thinking, and quick response to the environment.

Managing risk and resilience effectively requires multiple inputs and methods of modeling and analyzing risk and resiliency. This requires information gathering — risk intelligence — so the organization has a full perspective and can make better business decisions. Mature risk and resilience management is built on a cohesive and mature strategy, process, information, and technology architecture that can show the relationship between objectives, risks, controls, loss, and events.

This means maturing an integrated view of risk and resilience management that automates and makes processes 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 to enable not only resilience but also agility. Technology makes it easier to share data, while still maintaining independence of thought and action across the organization.

An integrated and mature risk and resilience strategy with common processes, information, and technology gets to the root of the problem. Leading organizations adopt a common strategy, framework, architecture, and shared processes to manage risk and resilience, increase efficiencies, and be agile in response to the needs of a dynamic and distributed business environment. Mature risk and resilience deliver better business outcomes because of stronger risk governance in context of the organization and its processes and objectives, which will deliver:

- **Efficiency.** Lower costs, reduce redundancy, and improve efficiencies.
- **Effectiveness.** Deliver timely, consistent, and accurate information.
- **Agility.** Improve decision-making and insight into what is happening across risks and operations.

Organizations need to be intelligent about what risk and resiliency management processes and technologies they deploy. A sustainable risk and resilience strategy means looking to the future and mitigating risk, as opposed to putting out fires. It requires that the following risk and resilience elements are in place:

- **Understand your risk.** An organization must have a risk-based approach to managing resilience and continuity of operations and services. This includes ongoing monitoring of risk in a dynamic environment as the business is continuously changing and so are its risks to strategy, operations, processes, and services. Risk assessments should cover exposure in specific processes, services, relationships, and geographies.
- **Approach resilience in proportion to risk.** How an organization implements risk treatment procedures and controls is based on the proportion of risk it faces. If a certain area of the organization or a business partner carries a higher risk of failure, the organization must respond with stronger resilience controls.
- **Tone at the top.** The risk and resilience program must be fully supported by the board of directors and executives. Communication with top-level management must be bidirectional. Management must communicate that they support the risk and resilience program. At the same time, they must be well-informed about the effectiveness and strategies for risk and resilience initiatives.
- **Know your business and who you do business with.** It is critical to establish a risk and resilience framework that catalogs risks, processes, and services. If there is a high degree of risk exposure, additional controls may be established in response. This includes knowing your third-party relationships as well as the organization is highly dependent on the extended enterprise to deliver goods and services.
- **Keep information current.** Risk and resilience assessment efforts must be kept current. These are not point-in-time efforts; they need to be done on a regular basis or when the business becomes aware of conditions that point to increased risk.

- **Risk and resilience oversight.** The organization needs a group who is responsible for the oversight of an integrated risk and resilience strategy. This requires a collaborative relationship where business continuity/resilience reports into risk management.

- **Established policies and procedures.** Organizations need documented and up-to-date policies and procedures that define risk and resilience responsibilities and processes. This starts with an enterprise risk management policy. These requirements and processes must be clearly documented and adhered to.

- **Assessment and continuous risk monitoring.** In addition to periodic risk assessment, the organization must also have regular risk and resilience monitoring activities to ensure that risk and resilience is understood in a dynamic context and how it impacts business processes, and services.

- **Manage business change.** The organization must monitor for changes that introduce greater risk and resilience issues. The organization must document changes that result from observations and investigations, and address deficiencies through a careful program of change management.

Five Stages of Risk and Resilience Maturity

Mature risk and resilience management is a seamless part of risk governance and operations. It requires a top-down view of risk and resilience, led by the executives and the board, where risk and resilience management are part of the fabric of business operations and processes - not an unattached layer of oversight. It also means bottom-up participation, where business functions identify and monitor risk and resilience that expose the organization. GRC 20/20 has developed the Risk and Resiliency Management Maturity Model to articulate maturity in the risk and resilience management processes and provide organizations with a roadmap to support acceleration through their maturity journey.

There are five stages to the model:

1. Ad Hoc
2. Fragmented
3. Defined
4. Integrated
5. Agile

1: Ad Hoc

Organizations at the Ad Hoc stage of maturity have reactive approaches to risk and resilience management at the department level. Businesses at this stage do not understand risk and exposure; few if any resources are allocated to risk and resilience. The organization addresses risk and resilience in a reactive mode — doing assessments when forced to. There is no ownership or monitoring of risk and resilience, and certainly no integration of risk and resilience information and processes in context of objectives, strategy, performance, and business change.

Key elements that identify an organization is at the Ad Hoc stage are:

- **Blind-spots.** Businesses at this stage are subject to many blind-spots. Understanding of risk and continuity is disconnected and not working together.
- **Reactive.** The organization addresses risk and resilience in a reactive, firefighting mode e.g., completing assessments when forced to.
- **Lack of ownership or accountability.** No one has been appointed to take control of risk and resilience.
- **Lack of process.** There is no defined or consistent processes or methodologies for managing continuity of processes and services or the risks that they are exposed to.
- **Under resourced.** Few, if any, resources are allocated to risk and resilience governance.

Characteristics of the *Ad Hoc* stage are:

- ❑ Siloed and Ad Hoc practices
- ❑ No structured and ongoing risk or resilience program
- ❑ Lack of skills and resourcing,
- ❑ No defined roles and responsibilities
- ❑ No governance structure of a risk management matrix in place
- ❑ No defined management program or risk framework
- ❑ No documented policies or procedures.
- ❑ Ad Hoc and reactive risk and continuity assessments
- ❑ Document-centric approaches
- ❑ Ad Hoc reactive approach that addresses issues as they arise
- ❑ Little to no technology in place
- ❑ No visibility, trending or analytics
- ❑ No board or senior management sponsorship

- **Manual.** Little technology support is in place and a reliance on spreadsheets and email, processes fail to be consistent.

Organizations in the Ad Hoc stage are very much in reactive mode and are likely to answer many of the following in the affirmative:

- Does risk and resilience program lack clear owners and accountability within departments and disconnected from each other?
- Are assessments and continuity plans put in place after the fact, when the organization realizes it is exposed or someone is insisting on them?
- Is risk and resilience largely undocumented, or trapped in silos of spreadsheets and documents?
- Does the organization lack any process, information and technology architecture to support risk management and business continuity?
- Does the department or business function have no ability to report and trend risk and resilience over time?

2: Fragmented

The Fragmented stage sees departments with some focus on risk management and business continuity within respective areas, but they are disconnected and not working together. Information and processes are highly redundant and lack integration. With siloed approaches to risk management and resilience (e.g., business continuity, disaster recovery), the organization is still very document centric. Processes are manual and they lack standardization, making it hard to measure effectiveness.

Key elements that identify an organization is at the Fragmented stage are:

- **Pockets of good practice emerging.** The organization may have some pockets of good practice emerging, but they need joining up.
- **Blind-spots.** Businesses at this stage are still subject to blind-spots, especially across the organization as so much information exists in departmental silos.

Characteristics of the *Fragmented* stage are:

- ❑ Tactical siloed approach to risk and continuity/resilience in different departments
- ❑ Starting to determine a roadmap, with pockets of good practice emerging
- ❑ Basic continuity plans and understanding of risk in place, and some standardization and qualification of risk
- ❑ Risk and resilience framework agreed but not implemented
- ❑ Risk and resilience governance and processes not fully embedded
- ❑ Processes are defined at the department level
- ❑ Some areas of risk management are in place but are not approached in an integrated or structured way
- ❑ No integration or sharing of continuity plans and risk between functions
- ❑ Reliance on fragmented technology and lots of documents
- ❑ Measurement and trending are difficult

- **Inefficient.** Departments may be working hard to address risk in silos, but without a full picture of risk there are duplicate efforts.

- **Disconnected.** Risk and resilience are addressed in a disconnected way in different departments. Disconnected across departments, disconnected across domains and disconnected across systems. Not only is this inefficient, but it also means risk can be exacerbated as it is not understood and addressed in context of the broader enterprise.

- **Manual.** With little technology support in place and a reliance on spreadsheets and email, processes fail to be consistent. This can slow your progress, with little ability to audit programs and activities.

- **Hard to measure and monitor.** While some data is beginning to emerge, it's in disparate systems and incomplete.

Organizations in the Fragmented stage of maturity answer many of the following questions affirmatively:

- Are risk and resilience/continuity activities tactical, disconnected from each other, and siloed?

- Does the organization lack an integrated risk and resilience approach across the organization?

- Is risk and resilience information scattered across various documents and technology sources?

- Is it difficult and time-consuming to track and trend risk and resilience information and reporting?

3: Defined

The Defined stage suggests that the organization has some areas of risk and resilience that are managed well at a department level, but it lacks integration to address risk and resilience across departments. Organizations in the Defined stage will have defined processes for risk and resilience in some departments or business functions, but there is no consistency. Risk and resilience processes have the beginning of an integrated information architecture supported by technology and ongoing reporting. Accountability and oversight for certain domains such as business continuity, disaster recovery, and/or enterprise and operational risk management are beginning to emerge.

Key elements that identify an organization is at the Defined stage are:

- **Better efficiency, but room for fine tuning.** There is a beginning to gain efficiencies at the department level as the organizations moves away from document and email centric processes but compiling reports across the business is likely to take time, and data is likely to be incomplete.

- **Semi-automated.** The organization is beginning to automate some business processes, leading to better risk assessments, and other efficiencies in parts of your program.
- **Reporting is getting better.** Better reporting and monitoring at the individual level, but it is still hard to extract an enterprise-view of risk and resilience.
- **Governance and oversight are starting to develop.** There is some senior management engagement, and particular risk domains and continuity plans may be benefiting from an enhanced level of oversight.

Characteristics of the *Defined* stage are:

- Risk and resilience management program and processes are defined with roles and responsibilities at a department level, but not across departments
- A formalized approach is in place with the framework designed and monitoring practices in place at a department level
- Risk appetite and tolerance not yet well defined or aligned, although inherent risk assessments are maturing.
- Strategic approach to governing risk and continuity is happening at a department level, but not across departments and functions
- The organizations are addressing islands and areas of risks
- Some reporting and trending at a department level

- **Better vision and transparency.** Businesses at this stage are beginning to eliminate blind spots, with a more integrated view of risk and resilience. However, the organization is still limited in not seeing an enterprise view of risk.

Organizations in the Defined Maturity stage answer many of the following questions affirmatively:

- Does the organization have silos of mature risk and resilience processes at a department, geographic area, or business unit level?
- Do individual departments have defined risk and resilience strategy, process, information, and technology architectures?
- Can departments readily report and trend on risk and resilience within their point-of-view?
- Have departments removed reactive document-centric approaches?
- Is there clear accountability and responsibility for risk and resilience at a department level?

4: Integrated

In the Integrated stage, the organization has a cross department strategy for managing risk and resilience across departments and functions. Risk and resilience are aligned across several departments to provide consistent strategy, frameworks, and processes supported by a common risk and resilience information and technology architecture. The

organization addresses risk and resilience through shared processes and information that achieve greater efficiency and effectiveness. However, not all processes and information are completely integrated, and risk and resilience if focused on avoiding issues and not on agility.

Key elements that identify an organization is at the Integrated stage are:

- **Good vision and transparency.** The organization benefits from an integrated view of risk and resiliency, across departmental, regional and enterprise levels. There is a beginning to consider the implications of performance and agility.

- **Good efficiency.** Silos have been broken down across the organization. It is likely that the organization has seen risk assessment monitoring automated dramatically, and the line of business become more engaged, and all three lines of defense operating in a single cohesive strategy, process, and technology for risk and resilience management.

- **Reporting is robust.** Reports are comprehensive and delivered to management about multiple categories of risk associated with business processes and services. The organizations are beginning to collect data about the performance of the program which can contribute to continuous improvement and ROI/value conversations.

- **Fully auditable.** The program has a system with full audit capabilities, so the organization can understand every action that has been taken in the program and whom it has been done by, when.

Characteristics of the *Integrated* stage are:

- ❑ Strategic approach to risk and resilience across departments
- ❑ Governance model agreed at board level
- ❑ Standardized risk and resiliency management strategy implemented and adopted, with documented processes
- ❑ Risks are cataloged, mapped, and monitored according to agreed and understood criteria
- ❑ Robust process monitoring measures are in place
- ❑ Appropriate skill-set and resources, with roles and responsibilities allocated
- ❑ Key departments and executives are engaged and involved.
- ❑ Silos have begun to be eliminated
- ❑ Common process, technology and information architecture across the business
- ❑ Trending and reporting across the business

Organizations in the Integrated Maturity stage answer many of the following questions affirmatively:

- Does the organization have a risk and resilience strategy that goes across departments?

- Does the organization have shared processes for risk and resilience management?

- Does the organization have a shared information and technology architecture for risk and resilience management?

- Can the organization report and trend on risks and resilience across departments?

- Can the organization aggregate and understand risk and resilience across the business, its services and processes, and impacts on objectives and strategy?

5: Agile

At the Agile Maturity stage, the organization has completely moved to an integrated approach to risk and resilience management across the business that includes an understanding of risk and compliance in context of performance and objectives. Consistent core risk and resilience processes span the entire organization and its geographies. The organization benefits from consistent, relevant, and harmonized processes for risk and resilience management with minimal overhead.

Agility is the ability of an organization to move quickly and easily; the ability to think and understand quickly. Good risk and resilience management is going to clearly understand the objectives of the organization, its performance goals, and strategy, and continuously monitor the environment for 360° situational awareness to be agile. To see both opportunities as well as threats so the organization can think and understand quickly and be prepared to move to navigate to seize opportunities while avoiding threats/exposures to the organization and its objectives.

But that is not enough. We need agile organizations to avoid and prevent events, but we also need agility to seize on opportunities and reliably achieve (or exceed) objectives. Agility is not just avoidance of hazards, threats, harms. Agility is also the ability to understand the environment and engage to advance the organization and its goals. Organizations need to be agile and resilient. Risk and resilience management needs to be an integrated part of performance, objective, and strategy management to achieve this capability to enable situational awareness for this organization so it can seize on opportunity as well as avoid exposures and threats.

The Agile Maturity is where most organizations will find the greatest balance in collaborative risk and resilience management and oversight. It allows for some department/business function autonomy where needed, but focuses on a common governance model and architecture that the various groups in risk and resilience governance participate in. The Agile stage increases the ability to connect, understand, analyze, and monitor risk relationship and underlying patterns of impact on performance, objectives, and strategy - as it allows different business functions to be focused on their areas while reporting into a common risk and resilience governance framework and architecture. Different functions participate in risk and resilience management with a focus on coordination and collaboration through a common core architecture that integrates and plays well with other systems.

Key elements that identify an organization is at the Agile stage are:

- **Performance focused.** The organization has a fully integrated risk and resiliency program that aligns with performance and objective management of the organization.
- **Agile risk management.** The organization has now moved beyond just a focus on resiliency to looking at how risk management makes the organization agile to understand what is coming on the horizon and prepare the organization to seize opportunities while avoiding or minimizing negative risk events.
- **Opportunity management.** The organization is leveraging risk and resiliency management to look for opportunities and not just avoid or minimize hazards and harm.
- **Collaborative.** The organization understands, analyzes, and monitors risk relationships across different business functions in a common risk and resilience governance framework and architecture.

Characteristics of the *Agile* stage are:

- ❑ Comprehensive governance structure with periodic meetings with board and regular governance review meetings
- ❑ Risk appetite and tolerance thresholds well defined and understood
- ❑ Risk mapping and segmentation reviewed regularly in context of change
- ❑ Cohesion across the three lines model
- ❑ Able to identify areas of improvement and measure ROI for continual improvement
- ❑ Industry best practices understood and embraced
- ❑ Enterprise view of risk and resilience across the ecosystem of the business and the extended enterprise of third-party relationships
- ❑ Risk and resilience management is integrated into roles and responsibilities
- ❑ Risk and resilience have an integrated view of performance, objectives, strategy in context of processes and services
- ❑ Risk and resilience agility is seen as a differentiator and impacts brand
- ❑ Extensive measurement and monitoring of risk in the context of business strategy and objectives
- ❑ Board and senior management led engagement, senior management champions the program

Organizations in the Agile Maturity stage answer many of the following questions affirmatively:

- Is there a single risk and resilience management strategy for the entire organization that all departments participate in?
- Is risk and resilience management understood and monitored in the context of performance and aligned with business strategy and planning?
- Can the organization monitor and trend risk governance and performance?
- Does the organization have mature processes, information and technology implementations to support risk and resiliency management?

- Is there regular monitoring for improvement in risk and resiliency management?

Getting to the Head of the Class

Advancing Your Organization's Risk and Resilience Maturity

Organizations with risk and resilience processes siloed within departments operate at the Ad Hoc, Fragmented, or Defined stage. At these stages risk and resilience management programs manage risk and continuity at the departmental level, and lack an integrated view, with no gain in efficiencies from shared processes.

In the Integrated and Agile maturity levels, organizations have centralized risk and resilience oversight to create consistent programs around the world with a common risk and resilience processes supported by an integrated risk and resilience information and technology architecture. These organizations report process efficiencies reducing human and financial capital requirements, greater agility to understand and report on performance, risk and continuity, and greater effectiveness through the ability to report and analyze risk and resilience data. The primary difference between the Integrated and Agile stage is the integration of risk and resilience in the context of performance, objectives, and strategy aligned across the organization. Differences may be seen in top-down support from executive management, and when various risk and resilience functions align with strategy to collaborate and share information and processes.

Considerations for Moving From Ad Hoc and Fragmented to Defined

Departments at the Ad Hoc and Fragmented stage have siloed approaches to risk and resiliency management at the department level. This means no integration or sharing of program and related risk and resilience information, processes, or technology. An organization that sees itself at the Ad Hoc stage should skip the Fragmented stage, and plan to move to the Defined stage.

To move from Ad Hoc or Fragmented to Defined requires the department to reduce manual data integration and improve overall visibility into risk and resilience at the department level. Organizations should consider defining risk and resilience process and information architecture at the department level and implement technology to manage multiple risk and resilience initiatives cohesively.

Considerations for Moving from Defined to Integrated

Departments at the Defined maturity stage are in a good place to lead the organization in a risk and resilience strategy to the Integrated stage. They have a strategic approach to risk and resilience management at the department level, supported by mature risk and resilience processes that can be extended to other departments.

To move from the Defined to the Integrated stage requires a common process, information, and technology approach that spans multiple departments. Organizations can leverage risk and resilience insight to improve planning and strategic decisions. A common governance model for risk and resilience management is used across lines of

business, functions, and processes. The organization needs a common risk and resilience methodology and taxonomy. Organizations at this level report process efficiencies - reducing human and financial capital requirements, greater agility to understand and report on risk and resilience, and greater ability to report and analyze risk and resilience data.

Considerations for Moving from Integrated to Agile

The difference between the Integrated and Agile stages is primarily one of context. At the Integrated stage the organization provides a consistent approach to managing risk and resiliency in context of hazards and continuity. This is supported by an established risk and resilience process, information, and technology architecture. While risk and resilience are understood in the context of the business, it is still focused more on risk and continuity than performance and strategy. At the Agile stage, the organization has performance, strategy, and objectives setting the context to achieve greater ability to avoid issues and not just respond to events.

Achieving the Agile stage requires risk and resilience expectations set as part of the annual strategic planning processes. The organization has measured and monitored risks and resiliency metrics in the context of business strategy, performance, and objectives. There is shared data and technology about risk and resilience, as well as decision support, optimization, and business intelligence. The organization has integrated risk and finance data to drive performance, while mitigating risks and ensuring integrity across the organization's operations, services, and extended enterprise of third-party relationships.

Critical Elements to Measure & Improve Risk & Resilience Maturity

The mature risk and resilience program can be measured against critical elements across governance and oversight, people and engagement, process and execution, and information and technology.

Risk & Resilience Governance & Oversight

- Governance model is agreed at the board level and effectively communicated and supported across the organization
- Policies and procedure for risk and resilience management are fully documented and consistently applied across the organization
- Risk and resilience management framework is well defined
- Measurement and trending is now available at an enterprise view
- Risk appetite and tolerance is well defined and understood in context of objectives, processes, and services of the organization

People & Engagement

- Clear roles and responsibilities across the organization
- Skills and resources are being applied to programs
- A dedicated team is in place and recognized as a center of excellence
- Skilled subject matter experts engaged in reviews
- Training and development are embedded
- Resource is focused on strategic value-added components of the program rather than tactical components
- You may be outsourcing some industry standardized activities to shared services communities

Process & Execution

- Well defined and executed processes across the organization
- There is a single version of the truth for all risk and resilience information that is well-integrated with other business systems
- Risk assessment and monitoring processes are standardized and automated
- Segmentation and risk tiering is in place
- Clear view of inherent and residual risk at both the process and enterprise levels
- Applying a risk-based approach that incorporates critical risks and the long-tail impact
- Multiple risk categories being assessed for each department, process, and services
- Issue management is in place, and full tracking and remediation is taking place in a single system
- Ongoing monitoring is established, with changes in risk profiles automatically triggering the appropriate actions
- Clear view and controls for the extended enterprise
- Managing risk through business change

- Performance management fully embedded in the program
- Program improvement decisions are facilitated by robust data

Information & Technology

- Leveraging best in class risk and resilience management software
- Risk portal for assessments, document collection, issue management and collaboration to engage front-line and operational management and risk owners
- Leveraging risk intelligence content to support automated business processes, and to support enhanced decision making

Fundamental Steps to Establishing Your Risk & Resilience Strategy

To achieve the full benefits from an integrated risk and resilience strategy, GRC 20/20 recommends the following next steps:

- **Gain executive support and sponsorship of the risk and resilience strategy.** The organization needs to work in harmony on risk and resilience. Different groups doing their own thing handicap the business. Executive support is critical to align the organization.
- **Establish a dedicated cross-functional team focused on a common approach.** It is vital to dedicate a cross-functional team to oversee ongoing harmonization of risk and resilience processes, integration of information, collaboration across risk and resilience functions, and execution of the strategy. This group identifies strengths within existing functions and enables other areas to benefit from them. The goal of this team is to develop shared framework, processes, and information.
- **Define a risk and resilience framework.** Companies must document and prioritize processes and services. This includes defining who owns risk, the subject matter experts for risk, and which function or process monitors risks. Policies, controls, and issues must be mapped back to the framework.
- **Develop harmonized processes.** Key to success is identification of shared processes and information for risk and resilience across the enterprise. This includes identifying technology solutions to support integrated information and process architecture.

The Role of an Integrated Risk & Resilience Technology Architecture

Risk and resilience fail 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 technology architecture supports the overall strategy and processes.

With processes defined and structured, the organization can now get into the specifics of the architecture needed to support risk and resilience processes. The risk and resilience architecture involves the structural design, labeling, use, flow, processing, and reporting of risk and resilience management processes.

Successful risk and resilience architecture will be able to integrate information across systems and integrate with external risk databases. This requires a robust and adaptable information architecture that can model the complexity of information, assessments, interactions, monitoring, and analysis of information that integrates and manages:

- **Facilitate collaboration in risk and resilience.** Engage and collaborate across risk disciplines of operational risk, business continuity management, IT, cyber/information security, and third-party management.
- **Enable contextually relevant decision-making.** Streamline and engage the business with risk intelligence for decision making processes to facilitate risk-informed business decisions.
- **Align the strategic business environment.** Communicate risk and resilience in context of business strategy, objectives, risk appetite, as well as strategic decisions and projects.
- **Provide analytics and dashboards.** Deliver risk analytics that is intelligent through the triangulation of collected information across business systems, processes, and services that initiates remediation tasks when needed.
- **Provide 360° contextual awareness.** Understand and document interdependencies between services, processes, assets, third-parties, products, channels, and risks.
- **Understand and connect risk.** Provide a risk context to objectives, processes, and services and understand the overall risk environment including risk appetite, risks, and controls.
- **Define levels of impact tolerances.** Cleary define and monitor multiple levels of impact tolerances for services. These can be monitored for both customer and prudential impacts on the firm, as well as the wider financial system.
- **Document the organization.** Define and document key business processes and services in the organization
- **Communicate with stakeholders.** Communicate and engage key processes and services to external stakeholders, such as regulators, partners, and customers
- **Leverage templates and best practices.** The solution delivers best practice resilience methodologies to enable identification of services and assess resilience.

- **Conduct scenario analysis.** Define and model scenarios to assess the resilience of processes and services and measure the likelihood of triggering defined impact tolerances.

- **Capture lessons learned from events.** With the solution, an organization can capture and retain lessons learned from past operational failures to minimize the likelihood and impact of future events.

- **Monitor the internal and external environments.** Continuously monitor information feeds on emerging threats, trends, and patterns within the internal and external business environments to identify what needs proactive response.

- **Workflow and task management.** Manage workflow and tasks, including alerts on pending tasks that are soon due and escalation of missed tasks. This delivers automatic routing of actions through workflow to appropriate users.

- **Notifications.** Provides notification through emails and personalized dashboards to notify control stakeholders and others of tasks and exceptions with embedded links to actions and tasks.

GRC 20/20's Final Perspective

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

The Agile Maturity approach is where most organizations will find the greatest balance in collaborative risk and resiliency management and oversight. It allows for some department/business function autonomy where needed but focuses on a common governance model and technology architecture that the various groups in risk and resilience utilize. A federated approach increases the ability to connect, understand, analyze, and monitor risks and underlying patterns of performance in context of processes and services within the organization and across third party relationships, as it allows different business functions to be focused on their areas while reporting into a common governance framework and architecture. Different functions participate in risk and resiliency management with a focus on coordination and collaboration through a common core architecture that integrates and plays well with other systems.

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