April 2023

FNZ

Best in Class GRC in Risk & Resilience Management
Medium Enterprise

2023
Best in Class
Awards

CASE**STUDY**

Governance, Risk Management & Compliance Insight

The information contained in this publication is believed to be accurate and has been obtained from sources believed to be reliable but cannot be guaranteed and is subject to change. GRC 20/20 accepts no liability whatever for actions taken based on information that may subsequently prove to be incorrect or errors in analysis. This research contains opinions of GRC 20/20 analysts and should not be construed as statements of fact. GRC 20/20 disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. Although GRC 20/20 may include a discussion of related legal issues, GRC 20/20 does not provide legal advice or services and its research should not be construed or used as such.

Table of Contents

Dynamic, Distributed & Disrupted Business ... 4

- Providing 360° Contextual Awareness of Risk ... 5

FNZ ... 5

- Best in Class GRC in Risk & Resilience Management – Medium Enterprise ... 5
  - *Risk & Resilience Strategy* ... *6*
  - *Risk & Resilience Process* ... *6*
  - *Risk & Resilience Technology* ... *8*
- Benefits Archer Delivered to FNZ ... 8
  - *Efficient* ... *9*
  - *Effective* ... *9*
  - *Agile* ... *9*

FNZ Achieved Best in Class Risk & Resilience ... 10

GRC 20/20's Final Perspective ... 10

About GRC 20/20 Research, LLC ... 12

Research Methodology ... 12

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 organisations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

FNZ

Best in Class GRC in Risk & Resilience Management Medium Enterprise

Dynamic, Distributed & Disrupted Business

The complexity of business – combined with the intricacy and interconnectedness of risk and objectives – necessitates that the organization implement 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. Keeping risk, complexity, and change in sync is a significant challenge for boards, executives, and management professionals throughout all levels of the organization. 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.

Too often risk management is seen as a compliance exercise and not truly integrated with the organization's strategy, decision-making, and objectives that has a symbiotic relationship on performance and strategy. It leads to inevitable failure for the organization's risk management program, providing case studies for future generations on how poor risk management leads to the demise of organizations: even those with strong brands and reputations. 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 the resilience of the organization.

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

- **Dynamic.** Organizations are in a constant state of flux as distributed business operations and relationships grow and change with fluctuating strategies, technologies, and processes while strategic, financial, and operational risks also are evolving. Managing risk and business change on numerous fronts buries the organization when managed in silos.

- **Distributed.** 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.

- **Disrupted.** Organizations face a 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.

Providing 360° Contextual Awareness of Risk

Organizations need complete 360° situational awareness and visibility into objectives, operations, processes, and risks. 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 and how it impacts strategy and objectives. The organization needs visibility into objective and risk relationships across processes to be agile and resilient in the context of risk. This requires that the organization implement an enterprise view of risk identification, assessment, monitoring, and automation.

Organizations need to see the intricate intersection of objectives, risks, and boundaries across the business. This interconnectedness of risk and 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. This enables the organization to focus on the analysis of risk in the context of the organization, its strategy, and objectives.

The Bottom Line: 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. The goal is comprehensive insight into risk and resilience management to identify, analyze, manage, and monitor risk in the context of strategy, objectives, 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.

FNZ

Best in Class GRC in Risk & Resilience Management – Medium Enterprise

FNZ is a global platform opening up wealth. FNZ partners with the entire industry to make wealth management accessible to more people. Today, they are partnered with over 650 financial institutions and 8,000 wealth management firms, enabling over 20 million people across all wealth segments to invest in the things they care the most about, on their own terms. This new approach makes wealth more transparent, sustainable and personal, empowering millions of people to grow their wealth the way they want it.

FNZ is a rapidly growing global organization supporting multiple financial institutions and wealth management firms by providing the technology these institutions utilize to interact with their end customers. As a major supplier of platform services to the UK financial services industry, there was a need for increased controls and activities to deliver an operational continuity and resilience strategy to meet the Financial Conduct Authority's Operational Resilience regulations. The information that would be required to adhere to the common standards set by the regulation was tracked by FNZ through various data sources or excel spreadsheets, which made it harder to gain more insightful analysis of the data. It was clear that given the varying sources of data, metric computation, and versioning, the key capabilities that would be required to support the operational continuity and resilience strategy would need to be centralized to enable teams across the organization to operate within the same framework and standard.

To address these challenges, FNZ redefined their approach to risk and resilience management through strategy, process, and technology . . .

Risk & Resilience Strategy

In response to the Financial Conduct Authority's regulation, FNZ in (collaboration with KPMG) drafted the following approach to deliver operational resilience, which has several different strands:

- **Vision.** Proactively demonstrate resilience to clients and regulators, improve resilience culture within the firm, and improve continuity by enhancing safeguards in operations and platform.
- **Identify Services.** Categorize and identify important business services following industry standard criteria. These are business services or direct and indirect services that, in case of a disruption, would cause harm to the business and/or clients.
- **Resource Mapping.** Identify end-to-end processes and underlying resources and assets required to carry out the important services, including suppliers, people, IT infrastructure, cyber, and property.
- **Resilience Control and Assess.** Resilience controls and metrics needed to be developed to assess the resilience posture adequately and effectively within the firm.
- **Impact tolerances and Scenario Testing.** Impact tolerance statements had to be developed to assess whether critical services could be recovered within the established timeframe in case of disruption.
- **Remediate and Invest.** FNZ determined that any weaknesses would be reported, and investments would be made to strengthen the resilience of critical services.

Risk & Resilience Process

The following initiatives were put in place to support the capabilities required by the operational resiliency strategy:

- **Strategy and Operating Model.** The United Kingdom team created an operational resiliency team to have management and oversight of the firm's strategy, governance, and policies, ensuring that the resilience culture was adopted and appropriate resources would be deployed and trained across the organization.

- **Service and Management Assets.** Agreed on taxonomies, mapping to underpinning assets, and supporting management architecture for the overall services of the firm - including client-facing, enterprise-level, and intra-group services.

- **Supplier Management.** Ensured key third-party contracts were mapped to critical services and third-party supplier management was performed as per guidelines.

- **Service Resilience Assessments.** Developed a resilience control framework and metrics for IT, cyber, people, property, and suppliers - including consolidation and reporting to inform key investment decisions.

- **Management of Contractual Provisions.** Ensured that resiliency required provisions were included in third-party and intragroup agreements.

- **Resilience by Design.** Identified and managed emerging threats that could impact the resiliency of custody services.

- **Scenario Testing.** Collaborated with clients to develop end-to-end impact tolerances for important services and testing scenarios against severe but plausible identified cases.

- **Recovery Planning and Management.** Worked on improving recovery planning by leveraging existing BCP/DR/Cyber capabilities and expanding recovery playbooks and business impact assessments.

- **Tooling and Data Embedding.** Determined the structured and automated dashboards which would support resilience, the control framework, and service assessment monitoring, supported by a selected tool as well as supporting the development and embedding of the methodology.

Risk & Resilience Technology

FNZ listed the key, high-level, and functional requirements that would need to be supported by the tool supporting the operational resiliency strategy, which included:

- Ability to maintain users and user groups for FNZ resources that would need to have access to the tool to perform the tasks based on roles.
- Ability to visualize and report on data relevant to the user with drill down capabilities into their resilience assessment to establish root cause and support solution design.
- Manage the workflow for periodic refreshes of data mapping and control assessments to support embedding across the operating model.
- Serve as a repository for services and related hierarchies, as well as the management of relationships between services and related data entities.
- Ability to input, either by user or automated source, resource data from various sources (people, premises, supplier etc.) and store in a structured database.
- Enable the application of rules to aggregate service assessment data and generate portfolio level reporting.
- Ability to input, either by user or automated source, scenario testing data, internal and external threat intelligence data, and store it all in a structured database.
- Ability to send notifications to users to initiate workflow.
- Maintain a complete audit trail of the changes made and sign-off(s) to ensure governance and compliance.
- Maintain the repository for operational resilience controls and synchronization with an enterprise-wide risk management framework, including the ability to add, edit, and delete controls.
- FNZ were already using the tool to support the risk management framework, integration between risk management and resilience data was critical to support more informed decision making

Benefits Archer Delivered to FNZ

Using this approach FNZ is better placed to address any future disruptions that could cause harm to clients, the firm, or end customers. This enables FNZ to differentiate themselves by being early adopters of an integrated approach to risk, resilience, and ESG. Further, this provides the ability to proactively demonstrate resilience to clients and regulators, improve resilience culture within the firm, and improve continuity. This also allows them to truly understand their end-to-end processes, supporting resources, and assets (including suppliers, people, IT infrastructure, cyber, and property) required to carry out the important services.

This has made FNZ more efficient, effective, and agile…

Efficient

Integrating the risk and resilience programs helps FNZ to align on common risk, goals, and measures, which enables them to fine tune insurance estimates and capital reserve needs. This integration also enables FNZ to leverage resources and people versus duplicating them across programs, adding significant efficiency gains.

By truly understanding their end-to-end processes and supporting resources and assets required to carry out the important services, FNZ can zero in on what needs to be prioritized and made resilient. This makes them much more efficient and effective, versus casting a wide net across those elements that are not as critical or mission critical.

Effective

The increase in efficiency has helped FNZ to establish and oversee the operational resilience approach through clear communication with stakeholder, and has ensured that management has the resources and capabilities to set out and deliver a organizational-wide approach to risk and resilience. This helps enable the embedding of risk and resilience within the firm's culture, which further allows for FNZ's operational resilience strategy to make prioritization and investment decisions to transform the resiliency culture proactively.

On top of this, FNZ has leveraged real time data notifications and reporting capabilities to ensure key stakeholders are informed at the earliest time in case of issues, enabling the organization to share risk information with end clients in real time.

Agile

FNZ, by leveraging Archer's technology framework, has Identified and managed emerging threats that could impact the resiliency of customer services. By collaborating with clients to develop end-to-end impact tolerances for important services and testing scenarios against severe but plausible identified cases, they have improved recovery planning and continuity by leveraging existing BCP/DR/Cyber capabilities and expanding recovery playbooks and business impact assessments. This gives them the ability to ingest scenario testing data, internal and external threat intelligence data, and store in a structured database with automated dashboards that support resilience, the control framework, and service assessments monitoring.

FNZ Achieved Best in Class Risk & Resilience

GRC is an integrated capability to reliably achieve objectives [GOVERNANCE], address uncertainty [RISK MANAGEMENT], and act with integrity [COMPLIANCE]. Successful GRC strategies deliver the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment. GRC solutions should achieve stronger processes that utilize accurate and reliable information. This enables a better performing, less costly, and more flexible business environment.

GRC 20/20 has evaluated and verified the implementation of Archer at FNZ and confirms that this implementation has achieved a remarkable case study in how to address risk and resilience management with clear benefits achieved.

This approach is "best in class", and in that context GRC 20/20 recognizes FNZ and Archer with a 2023 Best in Class GRC Award in the Category of Risk & Resilience Management – Medium Enterprise (1,000 to 10,000 employees).

GRC 20/20's Final Perspective

These are the key elements that makes this case study at FNZ best in class for risk and resilience management:

- Integration with other frameworks such as Risk Management and Business Continuity
- Review Appetite and Policy development within the firm to ensure resiliency culture is adopted across the organization and to improve the overall resiliency posture across the organization.
- Use of RCSA, ICAAP and Risk events outputs to inform scenario scope.
- Use of outputs from control testing to inform overall resiliency posture.
- Use outputs from Business Impact Assessments to inform Impact tolerance setting.
- Alignment to other regulations such as EBA guidelines on outsourcing and ICT management.
- Use intra group agreement approach to prove internal resilience posture.
- Ensure key controls are considered in the Supplier pillar and assessed from a service resilience lens.
- Use outputs of required supplier risk assessments and due diligence assessments to prove supply chain resilience posture.

- FNZ UK operational resilience requirements vs Global requirements and future proofing.
- Continual revision of strategy and framework as global requirements develop to ensure scalability.
- Ensuring Archer requirements are future proofed to easily integrate additional requirements.

FNZ wants to conduct risk quantification analysis, so they can monitor and report on their risk management programs with more actionable quantitative information. They also realize that risks are being treated across the company, and effective risk management is not confined to the role and responsibility of risk managers alone, so they need to focus on ways to coordinate risk practices and glean risk information from their business users. Finally, FNZ wants to integrate their environmental, social, and governance (ESG) with their risk and resilience programs to achieve a more aggregated view of the organization's risk, resilience, and ability to meet its social and sustainability responsibilities.

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
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com