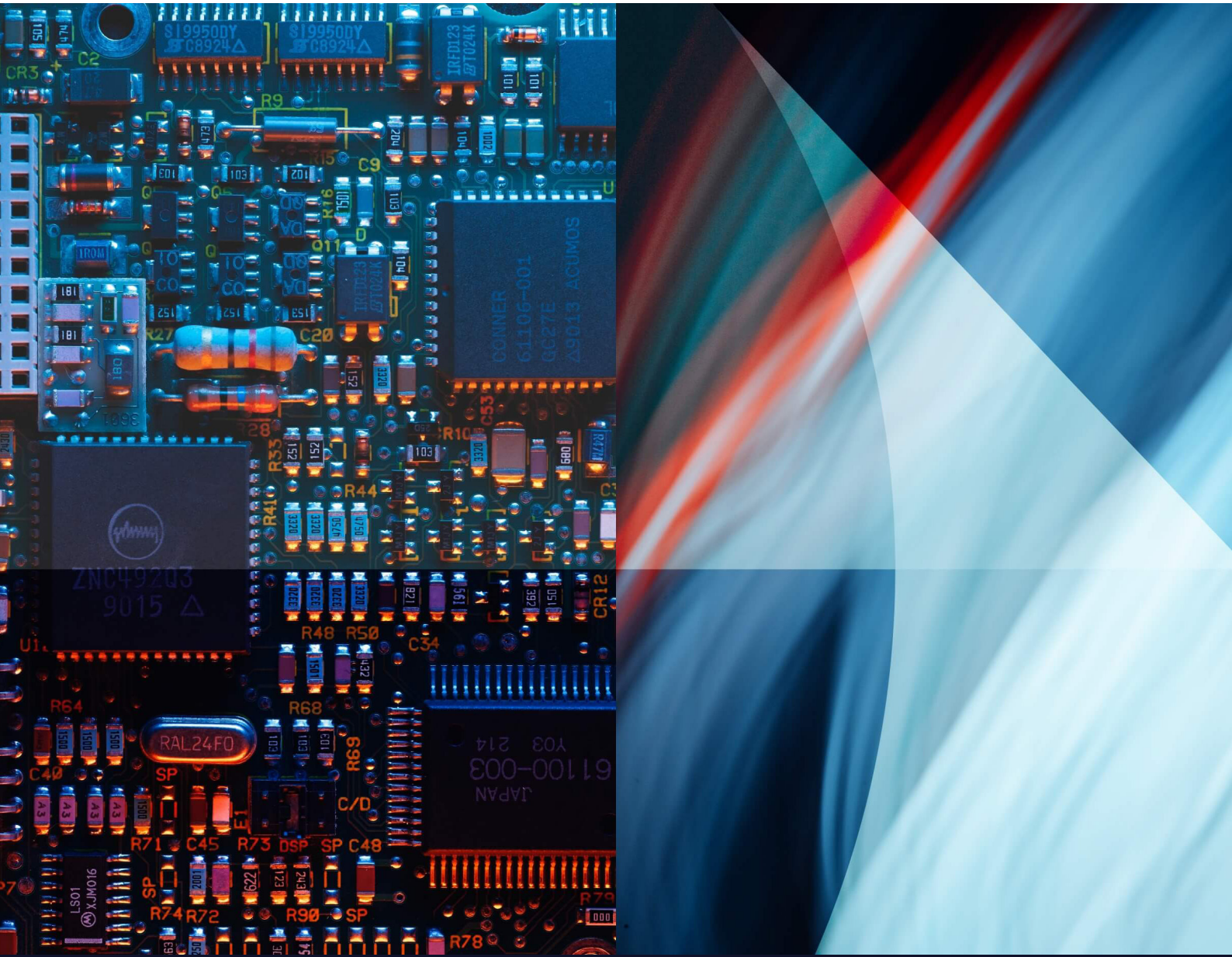
verdantix

Risk Management

Smart Innovators: Operational Resilience Software

By Elizabeth Babalola
With Bill Pennington

May 2024



Risk Management

Smart Innovators: Operational Resilience Software

By Elizabeth Babalola
With Bill Pennington

May 2024

Regulatory compliance, stakeholder expectations and the growing volatility of the risk landscape highlight the importance of operational resilience. Organizations are increasingly adopting digital solutions to tackle governance and data management hurdles. This report serves as a valuable resource for buyers seeking operational resilience software, offering a comprehensive benchmark of capabilities across 16 solution providers. It encompasses essential industry-agnostic capabilities for the future of operational resilience, namely, governance, risk management, ICT risk management, physical asset management, workforce and talent management, and supply chain management. Executives should use this report to evaluate vendors' capabilities across 12 key functionality areas, for informed decisions when purchasing operational resilience software solutions. In turn, vendors can utilize this report to enhance their solution capabilities and better meet evolving business demands.

Table of contents

Table of figures

Organizations mentioned

4C Strategies, Archer, Ascent Business, Bitsight, Business Continuity Institute (BCI), Camms, Corporater, Fusion Risk Management, Interos, LogicGate, LogicManager, MetricStream, Mitratech, Noggin, Origami Risk, Protecht, Riskonnect, SAI360, ServiceNow.

Disclaimer

As an independent analyst firm, Verdantix does not endorse any vendor, product or service covered in our research publications, webinars and other materials. Verdantix does not advise technology users to select only those vendors with the highest ratings. Verdantix research publications consist of the opinions of the Verdantix research team based on its analysis of the market, survey data and review of vendor solutions. Verdantix disclaims all warranties, expressed or implied, with respect to this research, including any warranties of fitness for a particular purpose.

Digital solutions help businesses navigate pressures around operational resilience

The operational resilience software market, driven by the business, regulatory, technology and threat landscape, is a major strategic investment software segment for organizations (see Verdantix Best Practices: Managing Operational Resilience; and see **Figure 1**). The market is growing rapidly, due to an increasing awareness of the importance of resilience, coupled with the rising frequency and severity of disruptions. Verdantix defines operational resilience software as:

> *"Specialized solutions that enhance firms' foresight in predicting, preventing, withstanding, adapting to and rebounding from unexpected disruption and risks across various operational domains. It integrates features for governance, risk management (including information and communication technology (ICT) risk management), business continuity planning, incident management, workforce management, and supply chain resilience."*

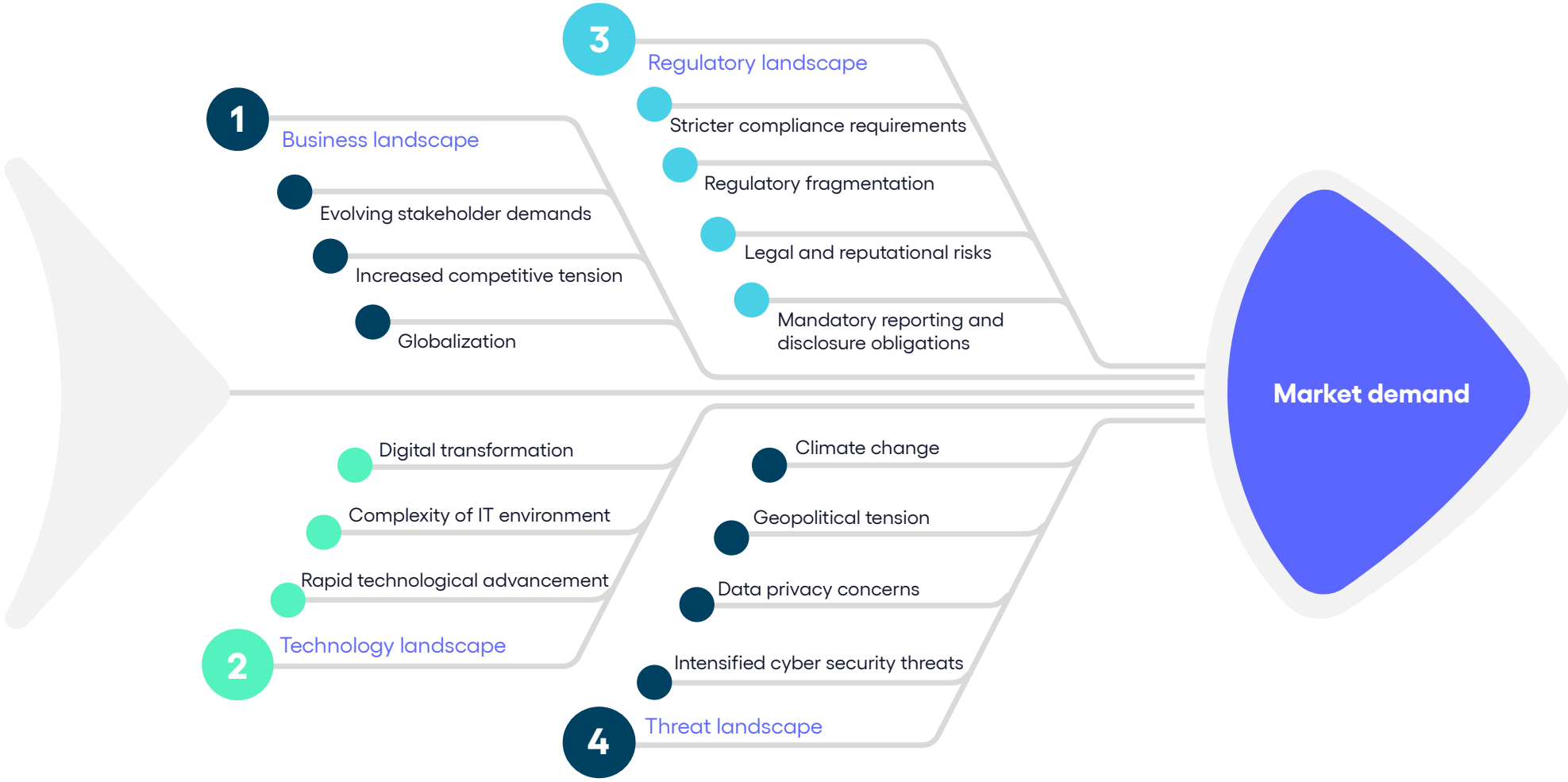
Keeping up with the pace of change in a shifting risk landscape is difficult

Organizations are under pressure from numerous sources, such as the global economy and market fluctuations, as well as from issues relating to corporate social responsibility (CSR) and sustainability. Alongside managing day-to-day operations, they must also ensure the resilience of their business operations. The successful development of strategic plans to address disruption and to implement operational resilience frameworks relies heavily on the leveraging of digital tools. While regulatory compliance has historically been the main driver for implementing operational resilience, market observations over the past two years indicate that organizations in non-regulated industries are also increasingly compelled to adhere to standards, due to evolving stakeholder demands. The challenges faced by firms are primarily driven by the rapid pace of change within the business environment (see **Figure 1**). Our research identified two main difficulties organizations encounter when planning and implementing operational resilience frameworks. These are:

- **Instituting appropriate levels of governance across their organization.**
  According to a survey conducted by the Business Continuity Institute (BCI) in 2023, embedding a culture within an organization that can support an operational resilience programme remains a key challenge to implementation. Digital tools are proven solutions to elevating governance effectiveness, with the ability to centralize governance, appropriately distribute responsibilities, and automate compliance monitoring across departments, to promote consistency and alignment with strategic objectives. The strengthening of a firm's risk awareness, culture and governance can be achieved by leveraging the real-time monitoring, strategic reporting and enhanced risk assessment capabilities provided by digital solutions.
- **Navigating the complexity of finding the right data and metrics across their business.**
  Based on Verdantix interviews with industry leaders and regulators in the operational resilience field, data fragmentation, low data quality, an inability to access real-time data, inconsistent data interpretation and ineffective analysis of data are key challenges to implementing an effective operational resilience framework. Organizations can surmount these obstacles through streamlined data collection and analysis processes, and via integration capabilities across other systems, thereby enhancing the capabilities of digital solutions for risk assessment and the identification of system vulnerabilities.

Figure 1

The demand for operational resilience software is driven by a variety of factors



Source: Verdantix analysis

Introducing the operational resilience software market

Vendors offering operational resilience software have diverse heritages. This report focuses on software providers with different capabilities, across a range of industries, analysing their solution offerings and assessing their capabilities. This section details our research inclusion criteria, explores the vendor landscape, and indicates core functionality for operational resilience solutions.

Evaluated firms and selection criteria

Verdantix reviewed the capabilities of over 50 vendors to produce a shortlist of 16 operational resilience software providers targeting firms' varying needs. Benchmarked vendors have:

- **A dedicated solution with functionality across at least four of the core capabilities.**
  Vendors included in this study offer solutions or modules catering to firms' governance, risk management, ICT risk management, physical asset management, workforce and talent management and supply chain management requirements. Profiled vendors have functionality spanning a minimum of four of these core capabilities.
- **Established market presence and reputation.**
  To ensure the reliability, viability, quality and relevance of the study, only vendors with demonstrated track records of consistently delivering dependable resilience and GRC (governance, risk and compliance) solutions are included.
- **Fifty employees or more.**
  This report focuses on well-established vendors with the organizational, structural and technological capabilities to address the resilience requirements of firms across various industries. To ensure effective solution delivery, all vendors within this study's scope have at least 50 full-time employees.

Vendors from a range of backgrounds target the operational resilience software market

The market offers a wider range of services beyond our selection criteria, which assist firms in implementing their resilience frameworks through specialized modules or as part of integrated solutions. These vendors vary from established industry leaders to emerging entrants. Some vendors have a heritage in more than one area. Our research reveals that operational resilience software is available from:

- **GRC solution providers.**
  Vendors with a GRC heritage are major players in the operational resilience software market, holding the largest share. They contribute massively to resilience solution development by leveraging their expertise in risk management, regulatory compliance and governance practices. Archer, Camms, Corporater, LogicGate, Mitratech, Origami Risk and SAI360 fall into this category. They utilize their understanding and in-depth coverage of organizational risk management frameworks, regulatory requirements and industry standards – integrated into resilience solutions – to help organizations effectively manage and mitigate risks across various domains.
- **Business continuity and disaster recovery specialists.**
  Vendors in this category, such as 4C Strategies, Ascent Business, Fusion Risk Management, LogicGate and Noggin, draw on their extensive experience and expertise in resilience to offer solutions that can effectively mitigate and manage disruptions. These vendors leverage their unique heritage to provide niche-based solutions tailored to the specific needs of organizations. Their solutions support firms as they navigate the complexities of risk management by enhancing risk assessments, developing customized resilience plans, identifying vulnerabilities and crafting response strategies, with an emphasis on continuous improvement.

- **Major technology and software developers offering risk management solutions.**
  Prominent technology and software vendors support firms' operational resilience requirements by offering solutions that ride the wave of automation and innovative technologies, such as AI and ML (machine learning). An example is ServiceNow, which harnesses its comprehensive suite of technology solutions to deliver customizable and flexible resilience solutions. Digital solutions allow organizations to centralize risk data and gain comprehensive insights into their firm-wide risk landscape through integration with existing systems, such as data storage systems, network infrastructure, cloud platforms, compliance and governance solutions, physical infrastructure monitoring tools, service management platforms and other relevant applications and middleware.
- **Third-party risk management (TPRM) providers with associated resilience solution offerings.**
  In our market analysis, we discovered that these firms make substantial contributions to resilience solutions by tackling the challenges of managing risks linked to external partners, suppliers and service providers. Vendors with TRPM offerings, such as MetricStream, Noggin, Protecht and Riskonnect, provide specialized software that excels in performing thorough vendor risk assessments, streamlining due diligence and vendor selection procedures, and crafting fit-for-purpose contractual agreements containing provisions for security controls and business continuity planning (BCP). Their solutions facilitate the ongoing monitoring and supervision of third-party relationships, incident response management and recovery, and adherence to regulatory requirements.

Core capabilities essential for building operational resilience

Due to growing systemic complexities, and a rapid pace of disruption, firms are encountering challenges in implementing robust operational resilience frameworks. Consequently, vendors must continuously innovate, developing functionality for organizations to seamlessly integrate into their IT infrastructure, to expedite their implementation efforts. Amid a wide array of vendor offerings, Verdantix has categorized the most important functionality into six core capability areas (see **Figures 2** and **3**). As firms aim to fortify their operational resilience frameworks, they will require solutions that can:

- **Aggregate internal and external data from various sources.**
  An unbroken operational resilience framework relies heavily on high-quality data, and the seamless execution of practices relating to these data, consistently maintained at peak performance (see Verdantix Best Practices: Managing Operational Resilience). Vendors are developing solutions to alleviate the challenges faced by firms in sourcing both relevant internal and external data, navigating the intricacies of defining operational resilience metrics, leveraging historical data for insights into the predictability (or otherwise) of events, and establishing a unified framework inclusive of third-party risk exposure – as provided, for example, by the Noggin resilience platform.
- **Comply with regulatory and mandatory frameworks.**
  The influx of operational resilience regulations over the past two years underscores the paramount importance of resilience in regulatory agendas. With a multitude of regulatory bodies, swiftly changing standards and complicated challenges stemming from interdisciplinary facets and globalization, compliance has become an increasingly daunting endeavour for organizations. Firms need solutions that can expedite their compliance efforts and validate their adherence to the latest regulations on an ongoing basis, as these evolve. An example vendor in this area is Archer, which provides a solution to monitor and track real-time regulatory updates by country and jurisdiction.

Figure 2

Operational resilience software capabilities map

Note: Business continuity planning (BCP)/disaster recovery planning (DRP)/incident management (IM).
Source: Verdantix analysis

- **Establish appropriate governance for risk management across a firm.**
  To achieve the accurate execution of policies and procedures, alongside establishing clear accountability, it is essential to incorporate appropriate levels of governance into existing organizational structures and frameworks. Firms have recognized the critical importance of this and are increasingly turning to technology to enforce the desired level of governance, culture and behaviours throughout their organizations. Vendors such as Corporater and SAI360, among others, deploy solutions that streamline governance processes and foster a culture that prioritizes compliance, accountability and ethical conduct at every level.

- **Incorporate third-party risk exposures.**
  In today's interconnected business landscape, firms increasingly rely on external partners, suppliers and service providers to support their operations. However, this introduces inherent risks, ranging from the threat of data breaches to the possibility of regulatory non-compliance. To effectively manage risks associated with third-party relationships, firms need advanced technologies that enable comprehensive monitoring, assessment, mitigation and real-time visibility into the activities and vulnerabilities of the players in their networks. ServiceNow, for example, deploys a mature TPRM solution with advanced vendor risk rating solutions and benchmarking features, to enhance vendor risk management. Another example is Fusion Risk Management's solution, which provides up-to-the-minute information for continuous financial and data breach detection.

Figure 3

Operational resilience software assessment criteria

	Sub-category	Assessment criteria
Governance	Policies and procedures	• Facilitates the development of policies and strategies by defining objectives, priorities and the overall approach to managing and mitigating operational risks • Establishes a culture of continuous improvement by regularly reviewing and updating operational resilience strategies, policies and procedures
	Regulatory compliance & reporting	• Enhances the alignment of an organization's operational resilience efforts with relevant regulatory requirements and industry standards • Supports the implementation of monitoring mechanisms to track key operational resilience metrics and indicators
Risk management	Risk indicators/risk register	• Provides a comprehensive overview of various risks that impact operational resilience, along with relevant details, such as their likelihood, impact, mitigating measures and status • Early issue detection functionality through the measurement of unusual patterns and observable metrics that provide information about the likelihood or presence of risks
	Risk assessments	• Evaluates the likelihood and potential impact of identified risks on business operations • Ability to identify and analyse vulnerabilities and dependencies across an organization's processes • Continuous monitoring of residual risks against risk appetite metrics
ICT risk management	ICT risk management & cyber security	• Implements measures to protect and minimize the impact of cyber threats, such as malware and phishing attacks on an organization's IT systems, networks and data • Establishes mechanisms for the timely detection of cyber security incidents
	Business continuity planning (BCP)/ disaster recovery planning (DRP)/ incident management (IM)	• Supports the creation of strategies and procedures to recover and restore IT systems and data after a disruptive event • Supports the continuous improvement of DRP processes through regular testing and exercises • Functionality that aids the identification, reporting and resolution of IT incidents, such as hardware failures, software glitches, cyber security incidents and other disruptions that can impact the normal operation of IT systems
Physical asset management	Physical asset register	• Supports the development and maintenance of a comprehensive inventory and the mapping of all organizational assets, including physical assets such as buildings and machinery
	Business continuity planning (BCP)/ disaster recovery planning (DRP)/ incident management (IM)	• Supports the processes of creation and documentation of business continuity plans, risk mitigation strategies and resource allocation and communication protocols • Provides real-time alerts during incidents for notification, response activation and timely updates

Figure 3 (continued) ↓

Figure 3 (continued)

Workforce & talent management	Workforce planning	• Functionality for skills alignment and demand forecasting to cover critical roles and responsibilities for business operations • Ability to support workforce scenario planning, adoption of flexible staffing models, and implementation of succession plans
	Security & emergency assistance	• Establishes effective communication during emergencies • Functionality for monitoring and tracking business and workforce exposure to potential threats • Capabilities for predictive analytics and risk assessment to proactively identify potential security threats and vulnerabilities
Supply chain management	Third-party risk management (TPRM)	• Ability to aggregate risk data to identify, profile, evaluate, govern and mitigate risks from external entities, for improved management of dependencies and vulnerabilities • Conducts risk assessments of suppliers • Facilitates compliance of an organization's supply chain with relevant regulations and standards relating to product quality, safety and ethical sourcing
	Vendor risk information provider	• Integration with external data sources as part of the information used in monitoring supply risk exposure

Source: Verdantix analysis

Innovative features from major and specialized players simplify the complexities of operational resilience

Based on our comprehensive market analysis, we observe that major solution providers maintain extensive coverage across all the essential functionality required to remain competitive in the operational resilience software market (see **Figure 4**). Meanwhile, specialized solution providers typically focus on specific capabilities, offering in-depth coverage of those areas. For instance, Interos primarily emphasizes TPRM offerings, while Bitsight concentrates on cyber security solutions. This strategic divergence highlights varying approaches within the industry, with major players prioritizing breadth of coverage to appeal to a wide range of clients, while niche providers emphasize depth in particular functionality to cater to specific resilience capabilities and industries. Amongst the many digital solutions available, there are key considerations for buyers when choosing a solution. Organizations should consider:

- **Their overall business objectives and strategic priorities.**
  An organization's journey – from its level of operational resilience today, to the level it aspires to in the future – should be the greatest influencer of its choice of software, with this determined through regular assessments of its local, industry and regulatory needs. The chosen software must align with the organization's strategic goals, and provide robust risk management capabilities and compliance support.
- **Existing technology infrastructure.**
  Compatibility with existing systems is fundamental for seamless integration, to efficiently source the relevant data, avoid duplications and minimize disruption to ongoing operations. The chosen operational resilience solution should complement an organization's technology infrastructure, leveraging its existing investments and avoiding the need for extensive overhauls. Firms should also evaluate the adaptability and scalability of the new solution, to accommodate evolving business and strategic needs.

Figure 4

Operational resilience software providers: capabilities assessment

	Governance		Risk management		ICT risk management		Physical asset management		Workforce & talent management		Supply chain management	
	Policies & procedures	Regulatory compliance & reporting	Risk indicators/risk register	Risk assessments	ICT risk management & cyber security	BCP/DRP/IM**	Physical asset register	BCP/DRP/IM**	Workforce planning	Security & emergency assistance	Third-party risk management (TPRM)	Vendor risk information provider
4C Strategies	◔	◑	◕	◑	◔	◑	◔	◕	○	◕	◔	◑
Archer	◕	●	◕	◕	◕	◕	◔	◑	○	◔	◑	◕
Ascent Business	◔	◑	◑	◑	◑	◑	◔	◑	○	◑	◑	◑
Camms	◑	◕	◕	◕	◑	◑	◔	◑	○	◑	◔	◔
Corporater	◕	◕	●	●	◑	◑	◔	◑	○	○	◑	◑
Fusion Risk Management	◑	◕	◕	◕	◑	◑	◔	◕	◑	◑	◕	◕
LogicGate	◕	◑	◕	◑	◑	◕	◕	◕	○	◔	◑	◑
LogicManager*	◕	◕	◑	◑	◕	◑	○	◑	◔	◑	◑	◑
MetricStream*	◕	◕	◑	◕	◕	◑	◔	●	○	◑	◕	◕
Mitratech	◑	◕	◕	◕	◑	◑	◔	◑	○	○	◑	◑
Noggin	●	◕	◕	◕	◕	◑	◑	◕	◑	◑	◕	◕
Origami Risk	◑	◕	◕	◑	◑	◑	◑	◑	◔	◕	◑	◕
Protecht	◕	◑	◕	◕	◑	◕	◑	◑	◔	○	◑	◑
Riskonnect	◕	◑	◕	◑	◔	◑	○	◑	○	◕	◕	◔
SAI360	◕	◕	◕	◕	◕	◑	◑	◕	◑	◑	◕	◑
ServiceNow*	●	◑	●	◕	●	◑	○	◕	◔	○	◕	◕

Innovative/leading functionality	●
Advanced/mature functionality	◕
Intermediate/developing functionality	◑
Basic/foundational functionality	◔
No demonstrated evidence	○

Note: *Indicates scoring based solely on publicly available information, without input from the vendor through questionnaires or briefings.
Note: **Business continuity planning (BCP)/disaster recovery planning (DRP)/incident management (IM).
Source: Verdantix analysis

- **Heritage of the solution provider.**
  A solution provider's heritage can serve as a valuable indicator of its capability, credibility and alignment with an organization's operational resilience objectives. A provider's expertise and understanding of the specific challenges and requirements within an industry can lead to tailored solutions that better address a firm's unique operational resilience concerns. A software provider's experience, record of accomplishment in the industry and reputation for innovation can prove a reliable source of insight and instill confidence in the reliability and effectiveness of its solutions.

More firms will adopt operational resilience solutions

The complexity of both risk management and the broader business operating environment is expected to steadily increase, driven by the evolution of risks, changing customer and stakeholder expectations, heightened regulatory scrutiny, and ongoing globalization efforts (see Verdantix Strategic Focus: Linking Risk Complexity To Digital Requirements). Organizations will require real-time analysis of both internal and external data, existing policies, operating procedures and implementation processes, to ensure continuous improvement. As a result, they will seek digital solutions that embrace cutting-edge innovations compatible with their current infrastructure and capable of swiftly adapting to evolving circumstances, to ensure they remain at the forefront of operational resilience.

Uncharted territories in operational resilience solutions will harm strategic implementation

In the operational resilience market, Verdantix observes mature capabilities such as the identification, assessment, prioritization and mitigation of risks across operational, financial, regulatory and reputational dimensions. Solutions with such capabilities also incorporate robust features for BCP and disaster recovery (DR), facilitating the development and maintenance of response strategies, along with incident management (IM) tools for the timely detection and resolution of disruptions. Additionally, compliance management tools ensure adherence to regulatory requirements. Notably, security features such as encryption, access controls and audit trails are emphasized, to safeguard sensitive information and mitigate cyber security risks, enabling organizations to proactively manage risks, maintain business continuity and enhance overall resilience. However, our analysis of the available solutions revealed certain areas where capabilities remain underdeveloped. We found that:

- **Workforce and talent management resilience software needs are still unmet.**
  Organizations face challenges in integrating data from disparate sources, such as human resources (HR) systems, performance metrics and skills databases. This hurdle is hindering comprehensive analysis for operational resilience and planning. While solutions such as those offered by Fusion Risk Management, Noggin and SAI360 meet intermediate forecasting needs and incorporate traditional linear projections, there is still a need for increased scenario planning capabilities, adaptability to workforce demands, and advanced predictive analytic capabilities – for improved simulations of future workforce needs, amidst evolving external factors, as well as for accurate succession planning.

- **Real-time visibility of asset management remains a major need in execution.**
  Organizations persist in using traditional asset registers, because innovative solutions leveraging the Internet of Things (IoT), radio frequency identification (RFID) and sensors for real-time monitoring and tracking throughout the asset life cycle are lacking. This gap presents challenges related to interoperability, impeding seamless data exchange and creating blind spots in intelligence on performance, maintenance history and lifecycle costs. Thus, there is a pressing need for data analytics and predictive maintenance algorithms to optimize asset management strategies. Innovative solutions that enhance real-time visibility, asset intelligence, interoperability and integration with risk management practices in physical asset management will revolutionize operational resilience for organizations.

- **Innovation gap in security and emergency assistance is an opportunity for growth.**
  Enhanced interoperability between security systems and emergency response protocols is essential, alongside the prompt dissemination of emergency notifications and seamless coordination and communication between stakeholders during crises. There is also a need for predictive analytics to anticipate security threats and emergencies, integrating emerging technologies such as AI and ML for proactive risk mitigation and incident management. Addressing these gaps with innovative solutions will not only broaden the operational resilience software market, but enhance the efficiency of operational resilience strategies.

verdantix

Independent insight and analysis

Our research is a trusted source for some of the largest and most innovative businesses in the world. With over a decade of reports, data and analysis, our subscribers have access to depths of insight that cannot be found elsewhere.

Whether you are implementing a leading-edge technology strategy, or developing the products and value propositions of the future, our analysis will help you futureproof your thinking.

Our expertise

Environment, Health & Safety

ESG & Sustainability

Net Zero & Climate Risk

Operational Excellence

Real Estate & Built Environment

Risk Management

Contact

Verdantix Ltd, 30 Stamford Street, London SE1 9LQ, United Kingdom

contact@verdantix.com

@Verdantix

Opportunities at Verdantix

Since 2008, Verdantix has been delivering high-quality research and advice to its clients. If you're interested in joining a world-class team with an unwavering focus on success, apply to join us today. We are delighted to be hiring across all teams and have a variety of opportunities in both London and Boston