

Tech Roadmap: Risk Management Technologies (2026)

By Tom Murphy
With Bill Pennington

April 2026



Tech Roadmap: Risk Management Technologies (2026)

By Tom Murphy
With Bill Pennington

April 2026

This report clarifies the business value, pace of innovation and maturity of 23 risk management technologies across four phases of the technology life cycle: Launch, Growth, Maturity and Decline. The technologies profiled include, but are not limited to, AI-powered internal compliance chatbots; AI-enabled regulatory change management solutions; risk management information systems; climate risk solutions; geopolitical risk intelligence platforms; agentic AI; operational resilience software; threat intelligence (cybersecurity) tools; third-party risk management software; governance, risk and compliance software; business continuity and disaster recovery solutions; data loss prevention solutions; financial risk management software; and claims management software. Risk management leaders, risk managers and budget-holders responsible for selecting technologies to support risk management processes – both within the enterprise and across the value chain – should use this report to identify technologies that can add value, as well as to explore options for pilot projects and to inform broader technology and digital strategies, to build effective risk management programmes. Risk-averse firms should focus on the potential of technologies with proven business value that are in the Growth or Maturity phases of the technology life cycle. Innovators and early adopters should take note of Launch-phase technologies.

Table of contents

Introducing the Tech Roadmap analysis	5
Key questions answered by the Tech Roadmap analysis	
Tech Roadmap analysis aligns with regulatory compliance and risk requirements	
Tech Roadmap for risk management technologies	6
Defining the market for risk management technologies	
Tech Roadmap methodology overview	6
Five market phases of technology maturity	
Three technology life cycles differentiate business value	
Technology adoption and success influence positioning	
Pace of innovation determines the time to the next lifecycle phase	
Risk management technologies in Phase 2: Launch	11
Geopolitical risk intelligence software	
Dark web monitoring solutions	
Agentic AI	
AI-powered internal compliance chatbots	
AI-enabled regulatory intelligence solutions	
Risk management information systems	
Risk management technologies in Phase 3: Growth	18
Climate risk solutions	
Reputational risk monitoring tools	
Operational resilience software	
Workforce risk software	



GRC software	
Third-party risk management software	
ESG reporting software	
Risk intelligence data tools	
Cyber threat intelligence platforms	
Risk management technologies in Phase 4: Maturity	28
EHS software: cloud	
Business continuity and disaster recovery solutions	
Claims management software	
Business process mapping	
Data loss prevention solutions	
Financial risk management software	
Whistleblower software	
Risk management technologies in Phase 5: Decline	35
Audit software	

Table of figures

Figure 1. Tech Roadmap terminology definitions	8
Figure 2. Tech Roadmap for risk management technologies	10



Organizations mentioned

3rdRisk, 4C Strategies, 6Clicks, A1 Tracker, Achilles, ACI Worldwide, Aclaimant, Actico, Adarga, ADP, Alcumus, AllVoices, Altares, AML RightSource, Anomali ThreatStream, apexanalytix, Apex EDI, APLANET, Appian, APP Tech, Arachnys, Aravo, Archer, Ascent Business, Association of British Insurers (ABI), AuditFile, AuditPRO, Aunetic, Aura, Avetta, Benchmark Gensuite, Bitsight, Bizagi, Black Kite, Bloomberg, BlueKanGo, Borable, BriteCore, Case IQ, Cato Networks, Certa, Check Point, CIPS, Circular IQ, Cisco, ClaimPilot, Clarity AI, CLDigital, ClickUp, Climate X, ClimateAi, ClimSystems, Compliance.ai, ComplianceQuest, ComplyAdvantage, CONFORMiT, Constella Intelligence, Cority, Corlytics, Corporater, CoSoSys, Creately, CreditRiskMonitor, Creditsafe, Crisis24, CSI, CUBE, CURA, Cybersixgill, CyberVadis, DarkOwl, Datadog, Dataminr, Decision Focus, Decisions, Digital Guardian, Diligent, Dior, DNV, Donesafe, Dow Jones, Dragonfly, Drova, Duck Creek Technologies, Dun & Bradstreet, DXC Technology, Ebix, Economist Intelligence Unit (EIU), EcoOnline, EcoVadis, Egress, Eightfold AI, Ellen MacArthur Foundation, Empowered Systems, Endpoint Protector, Enhesa, Enterprise Health, EQS, EQS Integrity Line, Equalture, ESG Playbook, Ethico, Ethixbase360, ETQ, Everbridge, Evotix, Exiger, FaceUp, Factual, Fathom, Featurespace, Feedzai, FICO TONBELLER, Fidelis Cybersecurity, FigBytes, FileTrac Evolve, FINEOS, First Street, Flare, Flashpoint, Forcepoint, Fortra, Fusion Risk Management, GAN Integrity, GIST Impact, Gloat, GOARC, Group-IB, Guidewire, HSI, Hyperproof, IBM, Ideagen, Identity Theft Resource Center, iGrafx Process360 Live, InfoTrie, Institute of Electrical and Electronics Engineers (IEEE), Insurity, Intel 471, Intellex, Intercontinental Exchange (ICE), International Organization for Standardization (ISO), Interos, INX Software, IPOINT, IsoMetrix, ISS ESG, JBA Risk Management, Jupiter Intelligence, KELA, KPA, Kroll, kShuttle, LexisNexis, LogicGate, LogicManager, LRQA, LSEG, Lucidchart, Majesco, Mandiant Advantage Threat Intelligence, MasterControl, McAfee, MCO (MyComplianceOffice), MetricStream, Micro, Microsoft, Milliman, Miro, Mitiga Solutions, Mitrastech, Moody's, Morgan Stanley, Morningstar Sustainalytics, Motorola Solutions, MSCI, Munich Re, Nasdaq, NAVEX, Ncontracts, Nestlé, Netskope, NICE Actimize, Nimonic, Nintex, Noggin, Novisto, OneTrust, Onspring, Open Corporates, Optro, Oracle, Orgvue, Origami Risk, Orpheus, Ortec Finance, Oversight Systems, Oxford Analytica, Pipefy, Plan A, Plan Brothers, Plural Policy, Polecat Intelligence, Position Green, Premium Continuum, Previsis, Prewave, ProcessUnity, Proofpoint, Pro-Sapien, Protecht, Quantivate, Quentic, RapidRatings, Recorded Future, Red Flag Alert, Regology, RepRisk, Resilinc, Resolver, Restrata, Revelio Labs, Resilience, Risk Intelligence, Riskconnect, RiskRecon, Riskthinking.AI, Route2 Sustainability, SAI360, Salesforce, S&P Global, Safetica, SafetyCulture, SafetyStratus, SAP, Searchlight Cyber, SecurityScorecard, Sedex, Seerist, ServiceNow, Signal AI, Signavio, Silobreaker, Simple But Needed, SmartSearch, SMS360, Screenshot, SOC Prime, SOCRadar, Solace Global, SpeakUp, Sphera, StandardFusion, StarTex Software, Supply Wisdom, SureCloud, Sust Global, Symantec, SymphonyAI, Taskforce on Climate-related Financial Disclosures (TCFD), TenForce, Teramind, Tesla, ThetaRay, ThirdPartyTrust, Threat Connect, Trend, Trulioo, TSC.ai, UiPath, UK Financial Conduct Authority (FCA), UKG, UL Solutions, US Securities and Exchange Commission (SEC), US Supreme Court, Vanta, Vault Platform, VelocityEHS, Ventiv Technology, Verizon Business, Visier, VisiumKMS, Volkswagen, Walor, WayCarbon, Whale, Willis Towers Watson (WTW), Wolters Kluwer, Workday, Workiva, Worklytics, World Economic Forum (WEF), Xapian, XDI Systems, Xybion, ZenGRC, ZeroFox.

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.



Introducing the Tech Roadmap analysis

With risk events and compliance demands intensifying, organizations are under pressure to adopt risk management solutions that address the full spectrum of threats. To support chief risk officers, compliance leaders and risk managers, Verdantix has applied the Tech Roadmap methodology to the risk management technologies landscape. Our report serves as an analytical tool to guide technology planning for corporate decision-makers and to inform product innovation for vendors.

Key questions answered by the Tech Roadmap analysis

The Tech Roadmap methodology provides a consolidated view into the maturity and business value of the solutions in a market ecosystem, using a standard graphic. It provides a dedicated, detailed profile for each of the technologies. The study analyses and addresses the following key questions for each technology assessed:

- **How mature is the technology?**
- **What is the technology's proven or predicted business value?**
- **How valuable will the technology be in the future?**
- **What is the technology's pace of innovation?**
- **Who are the key vendors?**

Tech Roadmap analysis aligns with regulatory compliance and risk requirements

Verdantix Tech Roadmap research assesses efforts by private-sector, public-sector and consumer firms to ensure effective risk management, organizational resiliency and regulatory compliance. It does so by:

- **Targeting risk management categories.**
The Tech Roadmap analysis identifies categories of products and services that address numerous aspects of risk management, such as compliance, governance and operational resilience, and which are specific to the everyday risk needs of generic firms. This helps profit and loss owners evaluate relevant technologies that align with their firms' risk management goals, risk appetites and budgets.
- **Seeking out innovative products and services.**
The risk technology landscape is constantly evolving, which means that executives aiming to enhance their firms' risk management efforts may struggle with a lack of expertise and understanding of the full range of market options. This can complicate the process of selecting and implementing the most suitable solutions. Beyond well-known technologies, the Tech Roadmap research process deliberately seeks out products that are in the early stages of their life cycles, from Research and Development (R&D) and into the early Launch phase. Risk decision-makers can utilize this information when developing their firms' digital strategies and roadmaps.
- **Identifying substitution opportunities.**
Risk-averse firms often continue using a product they are familiar with without fully considering alternatives and their associated opportunities and costs. The Tech Roadmap framework helps budget-holders explore substitute technologies that may provide expanded functionality, additional benefits or lower operating costs.
- **Including Decline as a phase in the technology life cycle.**
Investment decisions do not always account for end-of-life costs of products and services. The Tech Roadmap analysis identifies technologies that have progressed into the Decline phase and therefore pose business risks in terms of inefficiencies or a failure to meet the value promise, highlighting any identifiable replacement technologies.



Tech Roadmap for risk management technologies

The Verdantix Tech Roadmap analysis of risk management technologies helps executives and managers make better-informed decisions when identifying and comparing alternative solutions in the market. The analysis also helps vendors of risk management technologies understand the wider ecosystem of software solutions for various risk management use cases.

Defining the market for risk management technologies

This report focuses on technologies that support risk assessment and management. Verdantix defines risk management digital solutions as:

“Digital solutions that enable firms to identify, assess, monitor and take action to mitigate risks across their operations.”

The analysis focuses on, and explores in depth, technologies that support risk professionals and executives across industries in preparing for, and building resilience against, threats to business goals and operations (see **Figure 1**).

Tech Roadmap methodology overview

The Verdantix Tech Roadmap methodology identifies the level of market maturity for a technology and assesses its business value. This information, along with research and expert opinion, influences the positioning of an individual technology along the Roadmap (see **Figure 2**).

Five market phases of technology maturity

When analysing the technologies included in the Roadmap, Verdantix tracks a technology from its inception to replacement and retirement. As a technology matures, it advances through the phases of:

- **Research and Development.**
The first phase of technology maturity is Research and Development, which covers innovations that are being created in labs or by product development teams. The market presence of these technologies is in the form of small-scale pilots and prototypes: they are not yet commercially available. In this Tech Roadmap, we did not cover any technology in the Research and Development phase.
- **Launch.**
The second phase of technology maturity is Launch, during which technologies are launched commercially and vendors begin to demonstrate their tangible business value. Over time, the relative success of each technology becomes apparent, with some growing positively from this phase and others encountering challenges in the market. The success of any single technology depends both on its capabilities and its business value.
- **Growth.**
Following a technology's commercial launch, it typically continues along a product life cycle of high, medium or low proven value during the third phase of Growth. Technologies with high and medium proven value generate benefits that are sufficient for the ecosystem to grow rapidly, while technologies with low proven value, or those lacking a business ecosystem, decline rapidly.



- **Maturity.**

In the fourth phase, Maturity, a successful product or service has been widely adopted within the marketplace and maintains a significant customer base, with recurring revenues. In addition, there has been consolidation among vendors, and an entire ecosystem and value chain supports the continued purchase and use of the technology.

- **Decline.**

Technology moves into the final stage of the life cycle, Decline, as customers begin switching to more innovative substitutes. Customers either stop using the technology completely or replace it with alternatives.

Three technology life cycles differentiate business value

The Tech Roadmap analysis outlines and differentiates three distinct technology life cycles. Although this approach simplifies the complex nature of the evolution of products and services, it plays an important role in evaluating the potential longevity and future business impact of both emerging and current technologies.

The technology life cycles are:

- **Short-lived success followed by obsolescence.**
- **Proven success and moderate business value.**
- **Rapid success and high business value.**

Technology adoption and success influence positioning

Verdantix analysts place technologies on the Tech Roadmap graphic using a combination of evidence provided by research findings and the expert opinion of the Verdantix team. To determine each technology's placement, Verdantix considers the following key questions:

- **Is the technology commercially available?**
- **What is the scale of the leading vendors?**
- **How much investment capital is supporting the technology growth?**
- **What evidence is there of growing customer demand?**

Pace of innovation determines the time to the next lifecycle phase

Understanding a product or technology's current level of maturity, and the pace at which it is expected to progress, is essential for various stakeholders in the market. This insight supports decisions around factors such as time-to-market, adoption rates, alternative solutions and necessary investment. Tech Roadmap evaluations rely on consistent criteria to establish the time to the next phase of each technology. To develop these timelines, Verdantix poses the following questions:

- **How long has the product been in development or use?**
- **What are the pros and cons associated with the technology?**
- **What has been the customer interest in and demand for the technology?**
- **Are there any substitutes available or in development in the market?**



Figure 1
Tech Roadmap terminology definitions

Launch	Definition
Geopolitical risk intelligence software	Geopolitical risk intelligence (GRI) software leans on wider risk intelligence frameworks such as security/threat intelligence, supply chain risk analysis, and enterprise risk management (ERM) intelligence, to focus on risks related to international events, political instability and conflict, and their impact on persons, operations and physical assets. While some similarities are shared between GRI, economic risk intelligence and country risk monitoring, a key difference in GRI platforms is the primacy of state and conflict-driven catalysts – i.e sanctions, border closures, political violence, military escalation, government-sponsored information blackouts or nationalization – and the ability of the software to translate these into location and time-sensitive insights.
Dark web monitoring solutions	Dark web monitoring solutions (DWMs) are cybersecurity intelligence solutions that search and monitor hidden online ecosystems to detect where specific information appears. Most tools primarily search for exposed, leaked or illegally traded sensitive data held on Tor sites and illicit forums and marketplaces, via automated collection, indexing and AI-assisted pattern matching. These tools allow users to identify where their organizations' data have surfaced in underground and/or criminal channels, and to trigger the most effective remediation actions.
Agentic AI	Broadly speaking, agentic AI refers to AI systems that can pursue an end-goal defined by the user via autonomous planning, decision-making and execution. Differing from purely generative AI (GenAI) and from traditional automation and robotic process automation (RPA), agentic AI works by leveraging the processing power of large language models (LLMs) to perform broader actions within integrated systems. Agentic AI is commonly understood by industry leaders to be a subset of GenAI, representing a more action-oriented and operationalized form of the tool.
AI-powered internal compliance chatbots	AI-powered internal compliance chatbots leverage natural language processing (NLP) and machine learning (ML) technology to enable employees to ask about and more easily engage with a firm's policies, procedures and regulatory compliance information. The tool allows employees to quickly resolve common questions and navigate compliance issues within an organization, while maintaining data security and privacy within the internal network.
AI-enabled regulatory intelligence solutions	AI-enabled regulatory intelligence solutions use machine learning (ML) to automatically interpret regulations and permits, to determine appropriate regulatory requirements and action items. Specifically, AI leverages data scraping and natural language processing (NLP) to extract relevant data from external sources.
Risk management information systems	Risk management information systems (RMIS) combine insurance claims management with broader risk management capabilities. These solutions allow organizations – specifically, insurers and self-insured entities – to manage and track claims and incidents, assess risk exposure, analyse trends, manage insurance policies, optimize costs and support enterprise-wide decision-making.
Growth	Definition
Climate risk solutions	Climate risk solutions are software or data products that enable firms to identify, model and take actions to address climate-change-related factors across acute and chronic physical risks, as well as transition risks.
Reputational risk monitoring tools	Reputational risk monitoring tools measure and provide insights into the risks to an organization's reputation from a variety of factors, such as compliance, ESG and sustainability, sanctions and litigation.
Operational resilience software	Operational resilience software encompasses specialized solutions that enhance firms' foresight in predicting, preventing, withstanding, adapting to and rebounding from disruption and risks across various operational domains. The software 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.
Workforce risk software	Workforce risk software (WRS) solutions are digital tools that help organizations monitor and mitigate risks related to talent attrition, skills gaps and employee engagement. By analysing workforce data and using predictive insights, WRS enables proactive decision-making, to align talent strategies with business needs.
GRC software	Governance, risk and compliance (GRC) software applications are designed to improve risk management by collecting and storing risk data, supporting risk management governance, monitoring compliance risks and performing analysis of risks across all business functions and at all organizational levels.
Third-party risk management software	Third-party risk management (TPRM) software enables firms to aggregate risk data, to profile, evaluate, govern and mitigate risks from external entities, helping business better manage their dependencies and vulnerabilities. Key third-party exposures can be influenced by cyber, ESG, economic and geopolitical changes.

Figure 1 (continued) ↓

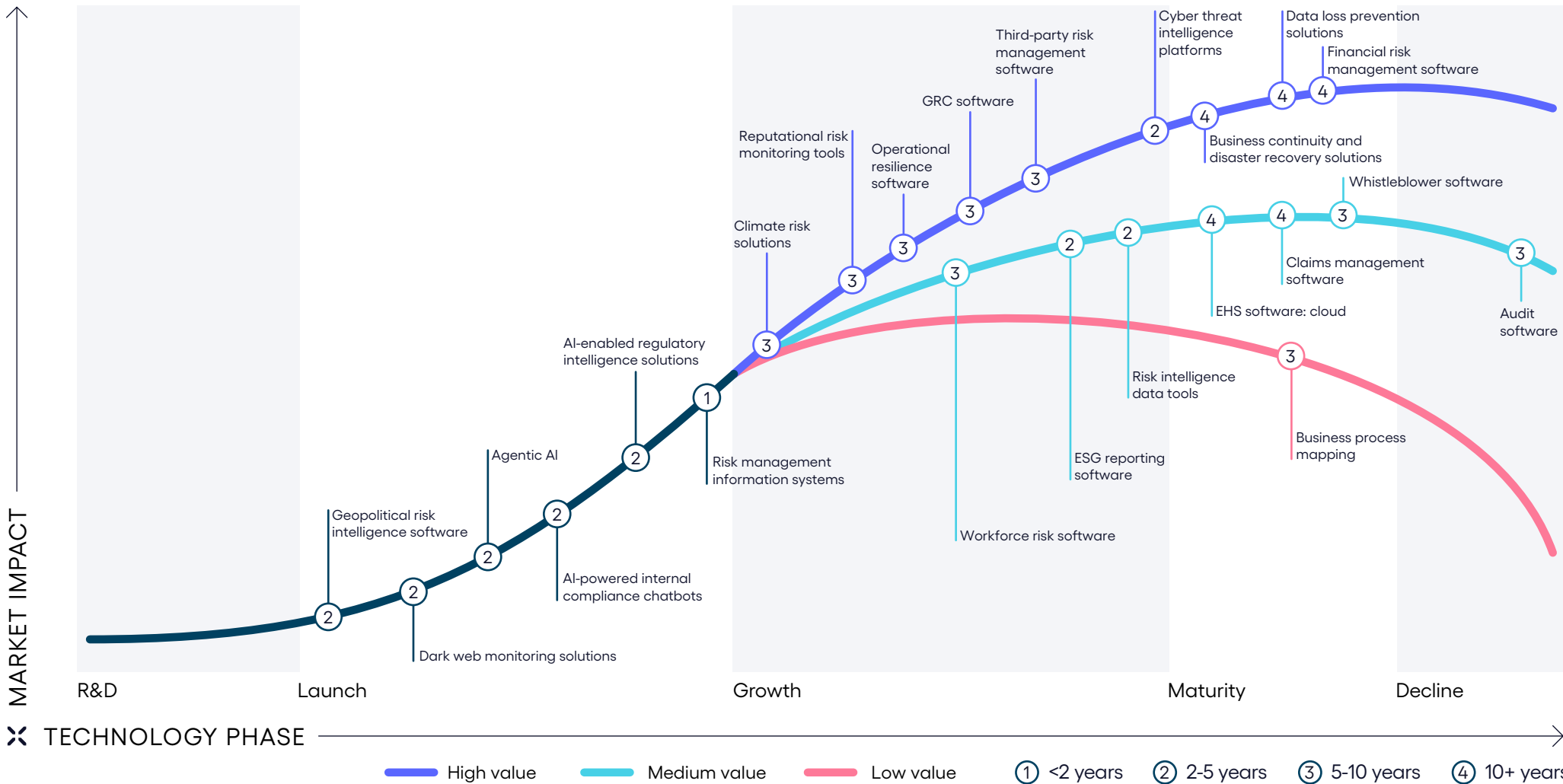
Figure 1 (continued)

ESG reporting software	ESG reporting software allows firms to collect, analyse and manage ESG information, to drive sustainability performance and report to mandatory ESG regulations and voluntary standards and frameworks. This covers ESG financial reporting (including double materiality), ESG risk management, impact assessment and sustainability reporting across ESG issues, within an enterprise and across the value chain.
Risk intelligence data tools	Risk intelligence data tools gather and feed real-time data to risk management providers, enabling the proactive identification and mitigation of risks in areas such as finance, cyber security, ESG, climate and reputation. By providing real-time data updates, risk intelligence data not only help organizations stay compliant and adapt to change, but allow them to analyse their impacts across an entire risk portfolio. Verdantix defines risk intelligence as “a combination of external data feeds, expert insights and/or technology to identify patterns, correlations and anomalies that could signal emerging threats.”
Threat intelligence tools (cyber security)	Cyber threat intelligence platforms (TIPs) collect, aggregate and analyse cyber threat data from both internal systems (e.g. logs and incidents) and external sources (such as threat feeds, the dark web, and information sharing and analysis centers (ISACs)). They provide actionable intelligence on threat actors, indicators of compromise (IOCs) and attack tactics. TIPs support security teams in detecting, prioritizing and responding to threats and can integrate with tools such as security information and event management (SIEM) and security orchestration, automation and response (SOAR) platforms for broader risk mitigation and incident response.
Maturity	Definition
EHS software: cloud	EHS software is a database-driven, firm-wide application that collects and manages data from areas such as environment, industrial hygiene (IH), occupational health (OH), medical administration, safety and waste management. A cloud-based EHS platform deploys the software on an external server, either for a single customer or for multiple firms (multi-tenant).
Business continuity and disaster recovery solutions	Business continuity and disaster recovery (BC/DR) software refers to digital tools and platforms that help organizations plan for, respond to and recover from disruptive events, such as cyber attacks, natural disasters and system failures. These solutions support the development of business continuity plans, automate incident response workflows and ensure that critical systems and data can be restored quickly, to minimize downtime. While business continuity focuses on maintaining operations during a disruption, disaster recovery centres on restoring IT infrastructure and data after the event.
Claims management software	Claims management software (CMS) is designed to streamline and automate the end-to-end process of handling insurance, legal or warranty claims. CMS provides organizations with tools to efficiently record, process, track and settle claims, while ensuring regulatory compliance, accuracy and transparency.
Business process mapping	Business process mapping is a digital tool that helps organizations visualize internal workflows and operations. It supports process standardization, identifies inefficiencies and risks, and serves as a foundation for automation, compliance and continuous improvement initiatives.
Data loss prevention solutions	Data loss prevention (DLP) technology encompasses solutions that provide visibility into data usage and movement, to address data-related threats, such as inadvertent or accidental data loss and sensitive data exposure. Critically, DLP works to enforce security policies for data at all stages, whether in use, in motion or at rest. This enables it to address data-related threats using remediation or warning features such as monitoring, alerting, quarantining and blocking suspicious or harmful activity.
Financial risk management software	Financial risk management software enables firms to identify, assess and continually monitor financial risks that can impact a firm's operations or profitability. Financial risk managers look for capabilities that target a range of issues, such as anti-money-laundering (AML) compliance, fraud detection and prevention, and credit scoring and assessments. The software is typically adopted by firms in high-risk data privacy industries, such as banking, insurance and healthcare.
Whistleblower software	Whistleblower software enables employees and third parties to securely and anonymously report misconduct, ethical violations or compliance breaches. It typically incorporates case management, secure intake channels and audit trails, to support internal investigations and regulatory compliance.
Decline	Definition
Audit software	Audit software automates governmental and industry-specific compliance protocols. Through automation, it analyses compliance documents, integrates data storage, accesses trend analytics, tracks audit trails, links audit management, and plans future audits internally. Audit software usually presents all data in a single platform and generates feedback reports to prevent and correct issues in the auditing process. IT security measures are included in most audit software, but to varying degrees.

Source: Verdantix analysis



Figure 2
Tech Roadmap for risk management technologies



Source: Verdantix analysis

Risk management technologies in Phase 2: Launch

Geopolitical risk intelligence software

Definition: Geopolitical risk intelligence (GRI) software leans on wider risk intelligence frameworks such as security/threat intelligence, supply chain risk analysis, and enterprise risk management (ERM) intelligence, to focus on risks related to international events, political instability and conflict, and their impact on persons, operations and physical assets. While some similarities are shared between GRI, economic risk intelligence and country risk monitoring, a key difference in GRI platforms is the primacy of state and conflict-driven catalysts – such as sanctions, border closures, political violence, military escalation, government-sponsored information blackouts and nationalization – and the ability of the software to translate these into location and time-sensitive insights.

Maturity phase: Launch. Early-stage GRI solutions have moved from pilots into scaled deployments, with a small but growing base and limited depth across use cases. Capabilities currently focus on core data ingestion, baseline risk scoring and automated alerting compatible with pre-existing risk workflows. GRI is continuously shifting away from pure reactive geopolitical crisis management towards proactive scenario planning and operational decision support. Elements such as configurable triggers are among the key enablers of this transition, whereby firms can translate geopolitical signals into pre-defined decision points that automatically reroute alerts to the right workflows. These signals may materialize as civil or military unrest close to physical assets, ground or air travel restrictions, and changes to partner continuity capacity. The integration of AI into GRI platforms is helping vendors ingest far higher volumes of open-source intelligence, particularly as the problem of signal abundance and noise remains a barrier to operationalizing geopolitical monitoring at scale. In the case of multilingual signals, while AI-enabled translations have managed to expand coverage beyond English-language reporting, for the examination of local updates and regional media, there is still some way to go to ensure that these translations are accurate across varying dialects and contexts.

Business value: High. The GRI market is currently sized at \$3.8 billion and projected to grow at a 10.30% CAGR to \$8.5 billion by 2033. As GRI software ultimately creates value by shrinking the time between a geopolitical change and an operational decision, international unrest is in part driving the current period of heightened adoption, although market value is not entirely dependent on this. As the technology assesses people, assets and operations together, and looks to translate geopolitical signals into time and location-specific impact pathways, GRI software is also proving useful for giving far more granular and context-rich risk surface analyses than broader third-party risk management (TPRM) platforms, particularly in unstable or conflict-adjacent regions. The value of the GRI market will likely rise due to the splintering of 'country risk' into a wider set of interconnected threat vectors; [the World Economic Forum \(WEF\) first Global Risks Report of 2026](#) indicates that these encompass geoeconomic confrontation, armed conflict, extreme weather, societal polarization and misinformation.

Pace of innovation: 2-5 years. Continued geopolitical fragmentation has pushed GRI vendors to innovate far faster than previously anticipated (see [Verdantix Strategic Focus: Trends, Developments And Capabilities Of Geopolitical Intelligence Vendors](#)). Within the remit of GRI, market segmentation shows a fairly even split across political risk intelligence, conflict monitoring, supply chain risk, economic sanctions tracking and country stability indexing. The 2025 Verdantix global corporate risk management survey, however, indicates that there remains a severe disconnect between threat perception and the reality of risk – with geopolitical risk consistently ranking low across risk significance, drivers of spending and perception of threat (see [Verdantix Global Corporate Survey 2025: Risk Management Budgets, Priorities And Tech Preferences](#)). At the organizational level, the GRI market appears to be driven by the need to detect and act on continuous geopolitical risk signals that are operationally disruptive, such as sanctions and export control changes, localized civil unrest and regime change. As a result, GRI tools are being increasingly optimized for picking up low-level, wide-spectrum signals that matter operationally. For example, in 2025, Crisis24 continuously monitored political unrest in Tanzania and utilized its pre-assessed routes to offer evacuation pathways for high-risk individuals. A good understanding of these signals is the basis for global risk

intelligence (see [Verdantix Market Insight: Understanding the Complexity of the Risk Intelligence Market](#)), with many leading GRI vendors duly focusing on linking niche signals relevant to business continuity.

Example vendors: Adarga, Crisis24, Dragonfly, Economist Intelligence Unit (EIU), Factal, Oxford Analytica, Prewave, Risk Intelligence, Seerist, Silobreaker, Solace Global, Sust Global.



Dark web monitoring solutions

Definition: Dark web monitoring solutions (DWMs) are cybersecurity intelligence solutions that search and monitor hidden online ecosystems to detect where specific information appears. Most tools primarily search for exposed, leaked or illegally traded sensitive data held on Tor sites and illicit forums and marketplaces, via automated collection, indexing and AI-assisted pattern matching. These tools allow users to identify where their organizations' data have surfaced in underground and/or criminal channels, and to trigger the most effective remediation actions.

Maturity phase: Launch. Due to the large scale and highly fragmented nature of the dark web, deployments in AI and machine learning (ML) have proven necessary to make DWM operational at scale. AI integration has been required primarily for the data collection phase of DMW, but is now also used to tackle the problems of duplication and noise. While the continued rise of cyber crime has certainly increased demand for DWM, it is important to note that most tools do not yet provide on-demand queried searches, but instead ingest continuous streams of data via external threat intelligence feeds and, in turn, create structured databases through which data can be matched. These external feeds may be either open-source intelligence or sourced from third-party providers.

Business value: Medium. The DWM market is [projected to grow at a 18.98% CAGR, up from \\$616.3 million in 2025, to \\$2.9 billion by 2033](#). The majority of DWM solutions are used in large enterprises, with the insurance, financial and banking industries leading the increase in adoption. The core use case is the ability to uncover compromised credit card information and other instances of financial fraud and to examine the digital environments in which this information appears.

Pace of innovation: 2-5 years. Because DWM indirectly deals with criminal networks, the pace of market innovation is constantly set by the fastest adversary. As bad actors have begun circumventing text-based detection by sharing data within images, Flashpoint's optical character recognition (OCR) platform has developed to see intra-image text and to identify where brand images and logos appear across datasets. The problem of signal abundance is unlikely to dissipate as adversaries gain ground, and it is therefore likely that the market will move towards more advanced incorporation into security operations in the coming years. Some vendors show signs of further integration already: Flare has integrated with Microsoft Entra ID to automate password resets when user credentials appear on known dark web logs, for example.

Example vendors: Bitsight, Constella Intelligence, DarkOwl, Flare, Flashpoint, Group-IB, Intel 471, KELA, Recorded Future, Searchlight Cyber, SOCRadar, ZeroFox.

Agentic AI

Definition: Broadly speaking, agentic AI refers to AI systems that can pursue an end-goal defined by the user via autonomous planning, decision-making and execution. Differing from purely generative AI (GenAI) and from traditional automation and robotic process automation (RPA), agentic AI works by leveraging the processing power of large language models (LLMs) to perform broader actions within integrated systems. Agentic AI is commonly understood by industry leaders to be a subset of GenAI, representing a more action-oriented and operationalized form of the tool.

Maturity phase: Launch. Operational agentic AI emerged as a force in the market after LLMs began to make natural language a practical control layer at the beginning of the 2020s. These early-stage generation and assisted workflows mostly operated as proto-copilots, with summaries and drafts failing to extend into complete workflow use. Integration with system-wide risk management platforms has grown since 2023, with a standardization of tool calling acting as the key enabler of agentic AI, completing more complicated tasks by allowing access to both internal and external assets. Since this development, agentic AI has shifted from being a mainly experimental tool to displaying more governed, workflow-native capabilities that allow outputs to be routed through specific playbooks, approvals and audit trails.

Business value: High. The market valuation of agentic AI was \$7.5 billion in 2025 and is forecast to reach \$199.5 billion by 2034, heavily driven by a push for autonomous execution across a range of software types, and a desire to reduce human-in-the-loop costs. Agentic AI creates value by compressing cycle times in workflows, with the ability to orchestrate multi-step work across systems and data sources. [In its 2026 global survey, the IEEE indicated](#) that mass adoption of agentic AI would accelerate through 2026, with 91% of respondents believing that its use for data analysis would continue to grow, and a further 47% expecting real-time identification of cybersecurity risks to be the top use case. Nevertheless, buyer concerns over possible over-valuations persist, in part due to staggering growth – CAGR projections have reached 43.8% for the period from 2025 to 2034 – and also because of the proliferation of agentic AI across the market in general. Concerns about a bubble are pushing vendors to reevaluate their operational playbooks by pivoting towards evidence-based deployment and by building model fungibility to reduce dependency on single providers (see [Verdantix Market Insight: AI Bubble Risk And Capital Cycles](#)).

Pace of innovation: 2-5 years. Agentic AI capability is moving quickly because it is ultimately anchored to the wider operating framework of AI, rather than existing as a standalone technology stack. Advances in models, systems integration and multimodal reasoning will continue to lift baseline performance. Governance is catching up, but remains uneven across the market, with many foundational governance frameworks still largely voluntary. Both the NIST Risk Management Framework and ISO 42001, for example, provide structured and risk-based guidance for system-wide use, but do not enforce compliance or penalties in the way that statutory regulation does. Nevertheless, shared principles appearing across leading frameworks – such as around accountability, transparency, human oversight, lifecycle documentation and continuous monitoring – seem to be converging on a baseline that buyers are increasingly translating into both procurement requirements and internal control libraries.

Example vendors: IBM, Microsoft, Salesforce, ServiceNow, UiPath.



AI-powered internal compliance chatbots

Definition: AI-powered internal compliance chatbots leverage natural language processing (NLP) and machine learning (ML) technology to enable employees to ask about and more easily engage with a firm's policies, procedures and regulatory compliance information. The tool allows employees to quickly resolve common questions and navigate compliance issues within an organization, while maintaining data security and privacy within the internal network.

Maturity phase: Launch. AI-powered internal compliance chatbots transitioned from the Research and Development phase in the mid-2010s to early market adoption in the 2020s, driven by significant advancements in AI and NLP technologies. Financial services and heavily regulated industries such as healthcare and insurance have been early adopters, but many firms still depend on manual processes and traditional compliance software. Integration with risk management platforms is limited, but growing. Most chatbots continue to rely on rule- or retrieval-based models, using pre-defined logic rather than deep AI-driven reasoning. Compliance bots powered by large language models (LLMs) are emerging to address this, but remain in the early experimental phases, facing challenges with accuracy, contextual understanding and regulatory interpretation – factors that have slowed widespread adoption.

Business value: Patchy/unknown. The business value of AI-powered internal compliance chatbots remains patchy and largely unproven, although early use cases show promise, particularly in financial services. These tools can enhance employee compliance by offering quick, accessible answers to routine questions, reducing reliance on compliance teams and improving response times. Advanced chatbots can guide users through document creation by collecting key information and ensuring regulatory accuracy, while their ability to update themselves with the latest policies and regulations helps minimize the risk of providing outdated guidance. Innovative applications, such as 3rdRisk's gamified chatbot for internal control testing, show the potential to boost engagement through features such as Microsoft Teams integration and incentive systems. Aravo, meanwhile, has recently unveiled its AI expert creator platform, on which a user can integrate specific ontologies and taxonomies into a widely customizable AI tool, which can, in turn, advise on aspects such as third-party compliance postures. Nevertheless, chatbots remain most effective when dealing with straightforward, frequently asked questions. Without sophisticated underlying technology, they struggle with complex, nuanced or multi-part queries – tasks still best handled by human experts. Trust also remains a barrier, with concerns around AI hallucinations and regulatory misinterpretations limiting their role in high-stakes compliance decisions. The 2025 Verdantix global corporate risk management survey confirms buyer reluctance when it comes to full adoption across internal AI systems: faith in AI judgment in the most critical use cases still lags (see [Verdantix Global Corporate Survey 2025: Risk Management Budgets, Priorities And Tech Preferences](#)).

Pace of innovation: 2-5 years. The pace of innovation for AI-powered internal compliance chatbots is set to accelerate as LLMs advance and organizations strengthen data governance. With improved training and fine-tuning on enterprise-specific data, chatbots are becoming more context-aware – able to understand user intent and organizational nuances with greater accuracy. Techniques such as retrieval-augmented generation (RAG) further enhance reliability by grounding responses in real-time, domain-specific data, while better data controls help ensure privacy and regulatory compliance. Despite these advances, widespread adoption will depend on regulatory acceptance, proven accuracy and seamless workflow integration. For now, chatbots are still narrow in scope and will remain a supplementary – rather than a primary – compliance tool.

Example vendors: 3rdRisk, 6Clicks, Aravo, Borable, MetricStream, NAVEX, OneTrust, Workday.

AI-enabled regulatory intelligence solutions

Definition: AI-enabled regulatory intelligence solutions use machine learning (ML) to automatically interpret regulations and permits, to determine appropriate regulatory requirements and action items. Specifically, AI leverages data scraping and natural language processing (NLP) to extract relevant data from external sources.

Maturity phase: Launch. AI-enabled regulatory intelligence solutions have been launched commercially, with a primary focus on increasing efficiency around meeting compliance requirements. They allow firms to automate elements of third-party and enterprise risk management (ERM) by interpreting regulations, suggesting relevant controls and continuously monitoring for compliance gaps – thereby reducing manual workloads and improving audit-readiness. As software vendors try to maintain pace with the complexity of regulations, the market has seen several acquisitions, such as that of regulatory intelligence platform Plural Policy by SAI360 in December 2025. There have also been developments around the processing and understanding of text across multiple languages and jurisdictions, with a growing number of vendors incorporating linguistic awareness into their models to avoid issues of mistranslation or misunderstood contexts. Certa, for example, has invested in advancing the multilingual capabilities of its platform to better understand linguistic nuances. Nevertheless, as AI use expands across the regulatory intelligence space, many solutions will struggle to keep pace with a growing language issue.

Business value: Promising. AI-enabled compliance holds significant promise and has seen increased adoption rates across high-risk industries where regulatory compliance is critical. Risk and compliance teams are turning to AI tools to automate regulatory change management, streamline policy updates and extract actionable obligations from complex legal texts. Solutions such as Compliance.ai (acquired by Archer in February 2024) automate the monitoring and analysis of regulatory changes across jurisdictions, using ML to map those changes directly to relevant internal policies and controls – dramatically reducing manual effort and the risk of oversights. Similarly, Wolters Kluwer's OneSumX Reg Manager leverages AI to track regulatory developments in real time and provide tailored, actionable insights to compliance teams. The result of solution adoption is improved efficiency, reduced wage overhead and a more agile response to regulatory developments, all of which translate into measurable bottom-line impact.

Pace of innovation: 2-5 years. The ability to streamline the time-intensive process of assessing documentation is a key driver behind the growing adoption of AI-enabled compliance solutions. According to Compliance.ai, such tools can save compliance teams an average of 174 workdays annually. However, concerns over data output accuracy persist, particularly when regulatory content is presented in complex or hard-to-parse PDF formats. As a result, firms should approach AI adoption with realistic expectations, recognizing the need for a blend of AI-directed control and human input, to reduce the likelihood of mistakes where there is low confidence surrounding an AI algorithm. As more risk and compliance software vendors look to leverage ML algorithms within their offerings, AI-enabled regulatory change management is poised to become a standard part of the compliance toolkit. This momentum also opens the door to the integration of AI-enabled compliance with robotic process automation (RPA) technology, offering further innovative use cases.

Example vendors: Archer (Compliance.ai), Certa, Corlytics, Corporater, CUBE, Diligent, Ideagen, Mitratesh, Nimonic, Regology, Wolters Kluwer.



Risk management information systems

Definition: Risk management information systems (RMIS) combine insurance claims management with broader risk management capabilities. These solutions allow organizations – specifically, insurers and self-insured entities – to manage and track claims and incidents, assess risk exposure, analyse trends, manage insurance policies, optimize costs and support enterprise-wide decision-making.

Maturity phase: Launch. The initial concept of RMIS emerged during the 1970s and 1980s, with systems primarily focused on digitizing risk and claims-related data, to replace manual processes and spreadsheets. While RMIS platforms have therefore been used for decades, the market has experienced significant consolidation over the past 10 years, with several independent vendors acquired by larger insurance and software firms, such as Riskconnect's purchase of Ventiv Technology in 2024. This wave of merger and acquisitions (M&A) activity has reduced competitive pressure, resulting in slower innovation and diminished momentum across the market. Core capabilities such as claims administration, incident logging and policy tracking have remained largely unchanged, and few vendors are actively expanding into adjacent areas, such as advanced analytics or third-party risk integration. This positions RMIS in the Launch phase – still relevant for core risk operations, but lacking the disruptive energy or forward-looking innovation seen in emerging risk tech segments.

Business value: Promising. RMIS software delivers promising business value by closing critical gaps in residual risk management and creating a centralized view across insurance, claims and operational exposures. Unlike traditional governance, risk and compliance (GRC) tools that stop at risk identification and scoring, RMIS platforms integrate claims data, exposure values and real-time incident tracking to support data-driven decisions on risk transfer and insurance optimization. This reduces the total cost of risk (TCOR) by aligning coverage more closely with actual risk profiles and enabling firms to negotiate lower premiums based on improved claims performance. While implementation complexity can vary across industries, the shift towards more user-friendly interfaces, scalable cloud deployments and embedded analytics signals a move away from patchy solutions towards systems that can bolster enterprise-wide risk programmes, with the technology set to become an essential tool for organizations seeking to proactively manage residual risks.

Pace of innovation: <2 years. The RMIS market is set to enter a Growth phase within the next two years, driven by rising claim volumes, mounting insurance costs and increasing demand for analytics. Reflecting the impact of these drivers, 35% of respondents to the Verdantix 2025 risk management global survey indicated plans to boost spending on RMIS software by between 10% and 24% from 2026 to 2027 (see [Verdantix Global Corporate Survey 2025: Risk Management Budgets, Priorities And Tech Preferences](#)). At the same time, innovations such as AI-powered incident intake, predictive analytics and real-time TCOR calculations are transforming RMIS into a proactive tool for cost reduction and risk prevention. Indeed, the 2025 Verdantix Green Quadrant for RMIS indicates both a demand and a need for the integration of AI and machine learning (ML) applications across RMIS, with several vendors – such as Archer and Origami Risk – standing out in this respect (see [Verdantix Green Quadrant: Risk Management Information Systems \(RMIS\) \(2025\)](#)). This convergence of market need and technological advancement positions RMIS for accelerated innovation and adoption (see [Verdantix Smart Innovators: Risk Management Information Systems \(RMIS\)](#)).

Example vendors: Aclaimant, Archer, Ebix, Origami Risk, Riskconnect.



Risk management technologies in Phase 3: Growth

Climate risk solutions

Definition: Climate risk solutions are software or data products that enable firms to identify, model and take actions to address climate-change-related factors across acute and chronic physical risks, as well as transition risks.

Maturity phase: Growth. Many software vendors initially developed climate risk solutions to help organizations align with the recommendations of the Taskforce on Climate-related Financial Disclosures (TCFD). With a recent increase in mandatory disclosures – such as the EU Corporate Sustainability Reporting Directive (CSRD) – and growing demand from stakeholders to understand firms' climate risk exposure, vendors have doubled down on reporting-focused solutions. Clarity AI offers software that auto-generates climate risk reports, while other vendors – such as Jupiter Intelligence and S&P Global – have been building out their capabilities to address the extensive CSRD requirements. With climate risks worsening, and businesses starting to show interest in climate adaptation, climate risk solutions are starting to deepen their offerings in other respects. Specifically, physical risks are taking an increasingly central role, pushing scenario analytics and asset-level exposures to the forefront of many platforms. Software vendors are also expanding their offerings to evaluate trade-offs between risk mitigation options and inform integrated risk management decisions (see [Verdantix Smart Innovators: Physical Climate Risk Solutions](#)). For example, XDI Systems provides off-the-shelf functionality to evaluate structural engineering interventions, and Resilience can assess the costs and benefits of strategic decisions such as entering into supplier contracts.

Business value: High. The regulatory landscape is shifting: the US Securities and Exchange Commission (SEC) voted to end the defence of the climate disclosure rules, while the EU's Omnibus proposal seeks to streamline the CSRD, the Corporate Sustainability Due Diligence Directive (CSDDD) and the EU Taxonomy. Nevertheless, the strategic importance of climate risk software remains high and investor pressure on asset managers to integrate climate-related risks into their investment processes is strong. A 2025 [study by Morgan Stanley](#) found that over 75% of institutional investors believe that physical climate risks will have an impact on asset prices between now and 2030, with [another 2025 study by the bank](#) showing that around 60% expect negative impacts from climate risks, on a physical level, over the next five years. There is a growing recognition among investors that climate-related risks have the potential to prompt market corrections, with these risks not yet fully reflected in asset prices. Climate risk is financial risk: solutions that support firms in assessing and managing this can help them mitigate damage from extreme weather, reduce supply chain disruptions, improve business resilience and avoid investments in long-lived assets that may be under threat.

Pace of innovation: 5-10 years. Despite the rollback of climate and ESG regulations across both the US and the EU, Verdantix research uncovers a reluctance to commit to firm-wide scale-backs (see [Verdantix Global Corporate Survey 2025: Risk Management Budgets, Priorities And Tech Preferences](#)). Buyers are mostly content with their current solutions; however, inevitably, growing risks will force software innovation (see [Verdantix Future Of Climate Risk Management](#)).

Example vendors: Bloomberg, Clarity AI, Climate X, ClimateAi, ClimSystems, EcoOnline, Fathom, First Street, IBM, Intercontinental Exchange (ICE), ISS ESG, JBA Risk Management, Jupiter Intelligence, Mitiga Solutions, Moody's, Morningstar Sustainalytics, MSCI, Munich Re, Ortec Finance, Resilience, Riskthinking.AI, S&P Global, SustGlobal, XDI Systems.

Reputational risk monitoring tools

Definition: Reputational risk monitoring tools measure and provide insights into the risks to an organization's reputation from a variety of factors, such as compliance, ESG and sustainability, sanctions and litigation.

Maturity phase: Growth. Reputational risk management tools have entered a Growth phase of their maturity curve, fuelled by heightened stakeholder scrutiny, regulatory pressure and the realities of digital transformation (see [Verdantix Strategic Focus: Innovations In Reputational Risk Management](#)). More intense examination from investors, consumers and regulators has elevated reputational risk to a top-tier concern: organizations are responding by embedding this into enterprise risk management (ERM) frameworks and adopting cross-functional approaches to manage these risks holistically. In recent years, the frequency and impact of reputation-related incidents have surged, with media observers noting that corporate crises are now an almost weekly event and often carry severe fallout. For example, in Q1 2025, Tesla reported a 13% year-on-year drop in vehicle deliveries – its weakest performance in nearly three years – amid backlash over CEO Elon Musk's political involvement. Renewed interest in reputational risk management is reflected in the market: in Q4 2025 [Signal AI secured \\$165 million in a high-profile growth-equity investment](#), with the funds aimed at accelerating product development and scaling expansion into the US and Europe.

Business value: High. Reputational risk management software holds high business value because it enables organizations to proactively identify, monitor and respond to threats that could damage brand perception and financial performance. A powerful example of the extent of the fallout that can stem from reputational risks was seen in 2025, with Dior's \$2.3 million settlement after an Italian investigation indicated substandard and unethical working conditions across several of the firm's third-party plants. While the payment was made in response to regulatory scrutiny and remediation expectations – with the proceeds going towards victims of labour exploitation – the episode demonstrates how quickly downstream supplier practices can become a brand issue. By equipping businesses with early-warning systems, real-time sentiment tracking and coordinated response tools, reputational risk software can help prevent or mitigate such crises, potentially saving millions in lost revenue, legal costs and long-term brand value.

Pace of innovation: 5-10 years. The pace of innovation in reputational risk software is relatively measured – set to unfold over the next five to 10 years – due to the complexity and breadth of the challenges these solutions address. Software providers are layering advanced technologies such as AI, natural language processing (NLP) and ESG metric integrations into already complex systems that must handle real-time data collection, risk scoring, regulatory compliance and stakeholder communication across a wide range of industries. Additionally, vendors are actively evolving their offerings by expanding AI use, refining crisis response templates and integrating deeper intelligence datasets – such as hyper-localized microeconomic forecasting to understand the ramifications of an economic downturn on local workforce conditions (see [Verdantix Strategic Focus: Mitigating Reputational Risks In Third-Party Risk Management](#)). These developments require careful testing, regulatory alignment and user trust, making innovation slower and more deliberate (see [Verdantix Smart Innovators: Reputational Risk Software](#)).

Example vendors: 3rdRisk, ComplyAdvantage, Dataminr, InfoTrie, Kroll (Resolver), LexisNexis, LRQA, LSEG, Mitrastech (Prevalent), Moody's, NAVEX, Polecat Intelligence, RepRisk, Signal AI, Supply Wisdom, TSC.ai, Xapian.



Operational resilience software

Definition: Operational resilience software encompasses specialized solutions that enhance firms' foresight in predicting, preventing, withstanding, adapting to and rebounding from disruption and risks across various operational domains. The software 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.

Maturity phase: Growth. Businesses are experiencing rapid changes in their operating environments, with operational challenges ranging from cyber attacks and supply chain disruptions to increasingly complex severe weather events. Manufacturers, service providers and vendors recognize the need to innovate quickly to maintain resilience and operational efficiency. Software firms have developed and launched digital platforms to help firms map their critical business functions, identify dependencies, boost their tolerance for disruption, improve crisis readiness, enhance communication using out-of-band communication tools, ensure regulatory compliance and minimize downtime during incident response. Operational resilience software vendors such as Corporater offer digital twin capabilities for scenario testing and planning, while Noggin brings a strong heritage in crisis management and incident response, with capabilities in real-time communication, incident tracking and resource management.

Business value: High. Operational resilience risks have grown significantly in recent years, driven by an increasingly complex threat landscape and rising regulatory pressure. Industries with globally distributed operations and critical business functions are especially vulnerable to disruption. In response to the surge in ICT-related threats, the EU introduced the Digital Operational Resilience Act (DORA) in January 2025, mandating financial entities and critical service providers to strengthen their digital defences. [A study by The World Economic Forum](#) (WEF) indicated that 77% of respondents saw an increase in cyber fraud in 2025, with these same risks extending into 2026 and showing no signs of slowing. The implementation of DORA underscores the urgency of safeguarding the EU's financial system from cascading digital disruptions, with businesses continuing to prioritize technologies that can proactively manage risks, ensure compliance and maintain continuity under pressure. The 2025 Verdantix global corporate risk management survey reflects the urgency of these drivers, with a collective 57% of respondents indicating that maintaining operational continuity is either their 'highest' or a 'high' risk priority in 2026 and 2027 (see [Verdantix Global Corporate Survey 2025: Risk Management Budgets, Priorities And Tech Preferences](#)).

Pace of innovation: 5-10 years. A major challenge for operational resilience software vendors is connecting the silos that exist in operational and technological infrastructure, as well as linking varying resilience strategies for different industries, based on operational processes and compliance requirements. Recent breakthroughs, such as resilience copilots, are equipped with application programming interfaces (APIs) to enable seamless integration into a firm's existing systems. However, they require lengthy trial and training periods. Increased connectivity on integrated platforms can also introduce new risks, such as accountability and data security, which must be addressed before the software is launched for data-sensitive industries (see [Verdantix Green Quadrant: Operational Resilience Software 2024](#)).

Example vendors: 4C Strategies, Archer, Ascent Business, CLDigital, Corporater, Drova, Fusion Risk Management, LogicGate, LogicManager, MetricStream, Mitrastech, Motorola Solutions (Noggin), Ncontracts, OneTrust, Origami Risk, Protecht, Restrata, Riskconnect, SAI360, ServiceNow.



Workforce risk software

Definition: Workforce risk software (WRS) solutions are digital tools that help organizations monitor and mitigate risks related to talent attrition, skills gaps and employee engagement. By analysing workforce data and using predictive insights, WRS enables proactive decision-making, to align talent strategies with business needs.

Maturity phase: Launch. Adoption is expanding as organizations seek to pre-empt workforce inefficiencies, skills shortages and talent attrition risks, amid labour market volatility and diversified hybrid/remote work models. A key driver of this growth is the ability of WRS platforms to merge both tangible and intangible data points – such as performance metrics, engagement levels and retention patterns – to generate actionable insights. By integrating these data streams across otherwise fragmented human resources (HR) functions, WRS supports more proactive and strategic workforce planning. For example, Aura's AI-assisted WRS solution extrapolates future internal skills gaps based on observed retention trends, helping firms align talent development with evolving business needs. ADP, meanwhile, uses its ADP DataCloud layer to benchmark firms against competitors in terms of employee performance. As organizations increasingly recognize the cost of misalignments between workforce capabilities and demand, the need for sophisticated, predictive tools has accelerated the maturity of WRS and fuelled its upward trajectory in the market.

Business value: Medium. While WRS delivers clear benefits in terms of improving talent planning, reducing attrition and identifying skills gaps, its business value is moderate, because it tends to impact operational performance more than core financial, compliance or reputational risk. Governance, risk and compliance (GRC) platforms, by contrast, address enterprise-wide risks – such as regulatory breaches, financial misstatements and third-party exposures – that can result in more immediate and severe consequences for a business. WRS is highly valuable for long-term workforce resilience and optimization, but its return on investment (ROI) is often more indirect, realized through improved productivity, employee retention and strategic workforce planning, rather than in terms of risk avoidance where there are high regulatory or legal stakes.

Pace of innovation: 5-10 years. WRS is likely five to 10 years away from full maturity. While innovation in AI, sentiment analysis and predictive modelling is driving rapid development, most workforce risk management today is still handled manually. Adoption is growing, but standardization across data inputs, ROI tracking and systems integration remains limited. With capabilities such as predictive attrition, skills gaps forecasting and real-time sentiment tracking continuing to evolve, we expect this technology to stay in the Growth phase until innovation slows and solutions become more embedded in overall enterprise risk strategy.

Example vendors: ADP, Aura, Eightfold AI, Equalture, Gloat, Oracle (Fusion Cloud HCM), Orgvue, Revelio Labs, SAP (SuccessFactors), UKG, Visier, Workday (Peakon), Worklytics.



GRC software

Definition: Governance, risk and compliance (GRC) software applications are designed to improve risk management by collecting and storing risk data, supporting risk management governance, monitoring compliance risks and performing analysis of risks across all business functions and at all organizational levels.

Maturity phase: Growth. GRC software is firmly in the Growth phase of the technology maturity curve, driven by a confluence of rising global risk complexity, expanding regulatory requirements and the digitization of enterprise risk management (ERM) operations. The software is experiencing healthy demand across sectors as firms confront an increasingly fragmented and shifting regulatory landscape, with businesses looking for centralized platforms to stay abreast of compliance and risk through one unified solution. To this end, 78% of respondents in the [Verdantix 2025 risk management global corporate survey](#) said that eradicating legacy systems and Excel-based processes was a 'moderate' to 'the highest' priority for their firm for 2026 and 2027 (see [Verdantix Global Corporate Survey 2025: Risk Management Budgets, Priorities And Tech Preferences](#)). At the same time, external pressures such as economic instability, geopolitical conflicts, climate risks and supply chain disruptions are converging, prompting organizations to prioritize a more holistic approach to risk management. The market is also seeing a significant boost from mid-market firms, which have traditionally lagged in GRC adoption, but are now accelerating investment thanks to the emergence of tailored and cost-effective software packages.

Business value: High. GRC solutions are of high value to businesses because they provide a structured framework for aligning operations with regulatory requirements, managing risk proactively and enabling visibility across the organization. By centralizing and automating GRC processes, these solutions reduce the likelihood of costly compliance violations, enhance decision-making with real-time risk insights and improve operational efficiency. They also foster a culture of transparency and resilience, enabling businesses to adapt quickly to regulatory changes and emerging threats, while maintaining stakeholder trust.

Pace of innovation: 5-10 years. GRC solutions are undergoing rapid innovation, mirrored by the fact that firms are more inclined to seek out platforms with purpose-built use cases that are highly applicable to their operational needs (see [Verdantix Green Quadrant: GRC Software 2025](#)). Advanced analytics is becoming a key area of innovation, with more mature firms targeting predictive risk indicators and intelligence integration to support proactive decision-making. To realize these capabilities and level of maturity, firms must embrace AI, small language models (SLMs) and data science tooling. Compliance automation and performance monitoring are additional areas of focus being bolstered by advancements in analytics, which can provide more strategic information about future changes. Despite these developments, it will take approximately five to 10 years for GRC solutions to reach full maturity, as customers work through challenges related to trust in AI, language models and advanced analytics. This timeline reflects the need to ensure that these new capabilities are not only effective, but secure, ethical and scalable across a wide array of customer contextual realities.

Example vendors: Archer, Corporater, Decision Focus, Diligent, Empowered Systems, Hyperproof, Ideagen, Kroll (Resolver), LogicGate, MetricStream, Mitrataech, NAVEX, OneTrust, Onspring, Optro, Origami Risk, Riskconnect, SAI360, SAP, ServiceNow, StandardFusion, SureCloud, Vanta, Wolters Kluwer, Workiva, ZenGRC.

Third-party risk management software

Definition: Third-party risk management (TPRM) software enables firms to aggregate risk data, to profile, evaluate, govern and mitigate risks from external entities, helping business better manage their dependencies and vulnerabilities. Key third-party exposures can be influenced by cyber, ESG, economic and geopolitical changes.

Maturity phase: Growth. The two primary factors driving the growth of the TPRM software market are the increasing complexity of supply chains and the steady increase in regulations requiring accountability across organizations' value chains. These dynamics have been complicated by enhanced volatility on a geopolitical level and uncertainty around US-imposed tariffs. In response, businesses have moved to rapidly restructure or diversify their supplier networks, often shifting sourcing to alternative markets with new and different types of risk and lower transparency. The US Supreme Court's decision on February 20, 2026 to strike down virtually all of the Trump administration's 2025 tariffs – and the administration's rebuttal by enacting the 1974 Trade Act to impose a 15% global base rate – expanded third-party risk for many firms, with sudden duty changes rippling through supplier pricing, logistics routes and contract terms. The likelihood of delivery disruption and margin erosion across third- and fourth-party networks has also been raised. The complexities of the situation are reflected in an increase in high-profile acquisitions in the TPRM space, such as Diligent's purchase of 3rdRisk in January 2026. To keep pace with current trends, many vendors are offering streamlined and thorough onboarding workflows: Ethixbase360, for example, provides enhanced due diligence and continuous monitoring across third-party networks, with a strong focus on anti-bribery and corruption, modern slavery and human rights, leveraging diverse data sources to identify red flags across ethics, integrity and responsible business conduct. An influx of other vendors has emerged in the space, with providers such as Decision Focus, Onspring and SureCloud offering competitive capabilities to meet customer requirements for rapid accessibility, scalability and user-centric support – all increasingly important features for the mid-market looking to quickly digitize TPRM programmes in turbulent times.

Business value: High. TPRM has become increasingly vital for businesses as they navigate a landscape where external partnerships are integral to operations. These third parties – vendors, suppliers and contractors – often have access to sensitive data and systems, making them potential entry points for cyber threats. According to a [2026 study by the Identity Theft Resource Center](#), 30% of all breaches involve at least one third party, with another [study by Verizon Business](#) noting that this figure represents a year-on-year doubling. Perhaps most crucially, the [World Economic Forum \(WEF\) Global Cybersecurity Outlook for 2026](#) indicates that 65% of large firms see supply chain and third-party vulnerabilities as the greatest threat to implementing effective cyber resilience – underlining the rationale behind board-level urgency on the subject. While the traditional functionality of supplier assessments remains a foundational component, the scope of TPRM platforms has significantly expanded in recent years. Today's solutions deliver high-value capabilities such as continuous risk monitoring, automated due diligence workflows and integration with external risk intelligence feeds (for example, cyber, ESG, financial health and geopolitical risk). They also support regulatory compliance by mapping third-party assessments to frameworks such as ISO 27001, NIST and the EU General Data Protection Regulation (GDPR), and provide centralized dashboards for tracking remediation and performance over time. As a result, TPRM platforms are increasingly seen as more than compliance tools, enabling strategic insight to reduce operational risk, improve supply chain resilience and strengthen enterprise trust.



Pace of innovation: 5-10 years. Ongoing geopolitical shifts – particularly in respect to escalating trade wars – along with regulatory developments and supply chain disruptions are forcing vendors to innovate far more quickly than previously anticipated. These developments have led to a significant broadening of firms' exposures, prompting vendors to accelerate the integration of real-time threat intelligence, AI-enhanced risk scoring and predictive scenario analytics into their platforms. Despite this momentum, both the technology and the organizations adopting it are still in a state of evolution, with [research by the WEF](#) indicating that only 33% of organizations have “comprehensively” mapped their third-party and supply chain ecosystems in 2026. As a result, TPRM software is not expected to reach full functional and strategic maturity for at least another five to 10 years, as firms continue to grapple with data integration challenges, evolving regulations and the need to scale risk management capabilities across increasingly complex global supply chains.

Example vendors: 3rdRisk, Achilles, apexanalytix, Aravo, Archer, Ascent Business, Avetta, Certa, Corporater, Decision Focus, Diligent, Empowered Systems, Ethixbase360, Exiger, Fusion Risk Management, GAN Integrity, Hyperproof, IBM (OpenPages), Ideagen, Interos, Kroll (Resolver), LogicGate, MCO (MyComplianceOffice), MetricStream, Mitratach, NAVEX, Ncontracts, OneTrust, Onspring, Optro, Origami Risk, ProcessUnity, Protecht, Resilinc, Riskconnect, SAI360, S&P Global (KY3P), SAP (Ariba Supplier Risk), ServiceNow, Sphera, SureCloud.



ESG reporting software

Definition: ESG reporting software allows firms to collect, analyse and manage ESG information, to drive sustainability performance and report to mandatory ESG regulations and voluntary standards and frameworks (see [Verdantix Green Quadrant: ESG & Sustainability Reporting Software \(2025\)](#)). It covers ESG financial reporting (including double materiality), ESG risk management, impact assessment and sustainability reporting across ESG issues, within an enterprise and across the value chain.

Maturity phase: Growth. ESG reporting software has seen widespread commercial adoption over the past five years, becoming a top priority for firms navigating both voluntary and mandatory ESG disclosures. While still a relatively new technology category, evolving regulatory requirements and growing stakeholder pressure for transparency have accelerated uptake. For risk professionals, ESG reporting tools are playing an increasingly critical role – not just for compliance, but as a means to manage emerging risks related to sustainability, supply chains, reputational exposure and climate impacts. As a result, firms are turning to digital ESG platforms to collect, analyse and contextualize the data needed for disclosures, as well as to support broader enterprise risk management (ERM) strategies.

Business value: Medium. ESG reporting software continues to play a significant role in supporting circular economy initiatives and improving supply chain sustainability – areas increasingly relevant to risk professionals. As compliance requirements evolve, particularly within the EU, firms must now report on circular economy metrics, such as those mandated by European Sustainability Reporting Standard (ESRS) E5 under the EU Corporate Sustainability Reporting Directive (CSRD). ESG reporting software automates data collection and reporting, helping firms manage complex supply chain data and ensure regulatory alignment. However, due to significant market volatility, ESG reporting tools are at risk of dropping down to a lower value. Specifically, tighter capital allocations and shifting priorities are pushing many businesses to revert to treating ESG as a compliance minimum. The 2025 Verdantix global corporate risk management survey showed that both ESG and sustainability initiatives are stalling, with the belief that ESG risk ‘is both material now and will become an increasing priority’ declining by 21 percentage points from our 2024 survey (see [Verdantix Global Corporate Survey 2025: Risk Management Budgets, Priorities And Tech Preferences](#)). The market is not actively in decline – the same survey indicates that only 7% of respondents are fully divesting from ESG measures – but is impacted by the unstable policy environment. Nevertheless, tools such as Circulytics continue to provide year-on-year tracking to support data-driven decision-making, while platforms such as Circular IQ’s CTI and the Material Circularity Indicator (MCI) from the Ellen MacArthur Foundation offer deeper insights into product lifecycle risks. Additionally, solutions such as CIPS’s activity-based costing (ABC) model help align circularity goals with risk-aware performance management. These capabilities are especially valuable as firms shift to circular supply chains with more distributed and dynamic risk profiles.

Pace of innovation: 2-5 years. In late 2024 Verdantix research found that the ESG reporting software market would grow to more than \$5.6 billion by 2029, at a CAGR of 26% (see [Verdantix Market Size And Forecast: ESG Reporting Software Solutions 2023-2029 \(Global\)](#)). However, following the EU’s proposed Omnibus simplification package – which aims to shrink the scope of the CSRD and reduce ESRS datapoints – already moderate growth has come to appear increasingly fragile, with buyers delaying or re-scoping ESG reporting software rollouts while they wait for clarity on thresholds and timelines. Nevertheless, solutions that quantify ESG impact – such as those offered by GIST Impact – are gaining traction, particularly as firms adopt double materiality assessments. For instance, Route2 Sustainability’s Value2Society tool converts a firm’s positive and negative ESG impacts into monetary values, helping organizations identify and prioritize the most effective actions.

Example vendors: APLANET, Benchmark Gensuite, CIPS, Circular IQ, Clarity AI, Cority, Diligent, Ellen MacArthur Foundation (Circulytics; Material Circularity Indicator (MCI)), ESG Playbook, FigBytes, GIST Impact, IBM, Intelix, IPOINT, IsoMetrix, kShuttle, Nasdaq, NAVEX, Novisto, OneTrust, Plan A, Position Green, Quentic, Route2 Sustainability, Sphera, UL Solutions, VelocityEHS, WayCarbon, Wolters Kluwer, Workiva.



Risk intelligence data tools

Definition: Risk intelligence data tools gather and feed real-time data to risk management providers, enabling the proactive identification and mitigation of risks in areas such as finance, cyber security, ESG, climate and reputation. By providing real-time data updates, risk intelligence data not only help organizations stay compliant and adapt to change, but allow them to analyse their impacts across an entire risk portfolio. Verdantix defines risk intelligence as “a combination of external data feeds, expert insights and/or technology to identify patterns, correlations and anomalies that could signal emerging threats” (see [Verdantix Strategic Focus: Dissecting The Dynamic Risk Intelligence Industry](#)).

Maturity phase: Growth. To manage growing risk exposures from expanding operations, new technologies and evolving risk landscapes, firms require real-time updates to analyse potential threats and mitigate risks. To address this, risk intelligence data platforms have launched software offerings that collect and report real-time risk data that impact customers in their respective industries. Customers can use these platforms to manage ethical third-party practices, cybersecurity risks, reputational risks and sustainability-related regulatory changes. Firms such as Black Kite provide third-party risk intelligence through technical cyber ratings and compliance correlations that rank a firm’s ability to meet regulatory requirements. As regulations such as the EU’s Digital Operational Resilience Act (DORA) continue to push businesses to enhance their operational resilience, risk intelligence data tools are on the rise, to help organizations keep up with regulatory changes in real time. Many firms are finding heightened business success by incorporating the tools into wider governance, risk and compliance (GRC) or supply chain management platforms, through which their intelligence feeds integrate with broader use cases.

Business value: Medium. Complex global supply chains, impending sustainability and ESG regulations, climate risks, reputational threats and cybersecurity issues are all drivers of demand for risk intelligence data tools. The Verdantix 2025 global corporate risk management survey revealed that organizations are continuing to make increased use of real-time data collection, regulatory intelligence feeds and geopolitical risk forecasting (see [Verdantix Global Corporate Survey 2025: Risk Management Budgets, Priorities And Tech Preferences](#)). However, while the adoption of risk intelligence feeds is growing rapidly, and is seen as increasingly important, the direct value of these feeds to businesses can be considered to be moderate, as they do not manage or mitigate risk on their own, but rather serve as crucial inputs that help shape broader digital risk strategies. The true utility of these feeds lies in their integration into platforms such as GRC and third-party risk management (TPRM) systems, where they can inform risk scoring, automate alerts and guide mitigation planning within a more governable risk management framework.

Pace of innovation: 2-5 years. With the integration of the AI-driven Internet of Things (IoT) into risk management platforms, for real-time data collection and processing, there is a growing focus on adapting Industry 4.0 advancements to further enhance on-demand data availability. The benefits of such integration and adaptations are reduced costs, through the earlier detection of risks, and a lower vulnerability to regulatory sanctions, as well as greater speed in the collection, analysis and delivery of data. Several risk intelligence data providers are already leveraging AI for data processing – witness EcoVadis implementing predictive intelligence into its data mining capabilities – with firms continuously innovating and integrating advancements into operational processes.

Example vendors: Altares, AML RightSource, Bitsight, Black Kite, CreditRiskMonitor, Creditsafe, CSI, CyberVadis, DarkOwl, Dow Jones, Dun & Bradstreet, EcoVadis, Exiger, LexisNexis, LSEG, Moody’s, Open Corporates, Orpheus, RapidRatings, Red Flag Alert, RiskRecon, SecurityScorecard, Sedex, Supply Wisdom, ThirdPartyTrust.

Cyber threat intelligence platforms

Definition: Cyber threat intelligence platforms (TIPs) collect, aggregate and analyse cyber threat data from both internal systems (for example, logs and incidents) and external sources (such as threat feeds, the dark web, and information sharing and analysis centers (ISACs)). They provide actionable intelligence on threat actors, indicators of compromise (IOCs) and attack tactics. TIPs support security teams in detecting, prioritizing and responding to threats and can integrate with tools such as security information and event management (SIEM) and security orchestration, automation and response (SOAR) platforms for broader risk mitigation and incident response.

Maturity phase: Growth. TIPs arose during the early 2000s after the sophistication of cyber threats rapidly increased. Today, vendors such as Datadog continue to advance their procedures for operational and strategic threat intelligence by leveraging increasingly vast datasets to better understand and respond to threats that have become highly organization-specific. As a central part of TIPs, firm-specific threat intelligence systems present the most space for growth, with a 2025 [World Economic Forum \(WEF\) report](#) showing that 49% of public-sector firms lack the internal capabilities to meet their self-imposed cybersecurity goals. One of the most pressing findings of the Verdantix 2025 global corporate risk management survey is the prevalence of cyber security as a key driver across three core risk categories: spending, threat perception and the materiality of risk (see [Verdantix Global Corporate Survey 2025: Risk Management Budgets, Priorities And Tech Preferences](#)). TIPs have excelled in the market by leveraging tailored anomaly detection platforms that learn a given network's normal behaviour patterns, to identify internal irregularities when they appear.

Business value: High. TIPs currently occupy a unique business position, particularly when considered in relation to the rapid development of AI. Not only are the risks of weaponized AI attacks pushing firms to consider TIPs, but vendors themselves are now required to constantly enhance the AI arm of their platforms, to maintain a strategic edge. The opportunity this challenge presents has boosted the market value of TIPs. For example, Cato Networks has recently expanded its AI system to monitor underground forums where weaponized AI is openly discussed, allowing AI-assisted machine learning tools (ML) to scrape, sort and summarize the development of malware techniques.

Pace of innovation: 2-5 years. Market expansion in this area is a result of many firms progressing through an extended phase of digital transformation and coming to rely more heavily on large language models (LLMs). Recorded Future is one example of a vendor seeking to meet their needs through the recent launch of its AI-enabled Autonomous Threat Operations platform. This auto-correlates a range of third-party threat feeds to provide a clearer picture of developing risk, reducing manual input. Overall, continued sustained growth in the use of AI solutions is securing innovation in the TIP space.

Example vendors: Anomali ThreatStream, Cato Networks, Cybersixgill, Datadog, Flare, Group-IB, Intel 471, Mandiant Advantage Threat Intelligence, Recorded Future, Seerist, Signal AI, SOC Prime, Threat Connect.



Risk management technologies in Phase 4: Maturity

EHS software: cloud

Definition: EHS software is a database-driven, firm-wide application that collects and manages data from areas such as environment, industrial hygiene (IH), occupational health (OH), medical administration, safety and waste management. A cloud-based EHS platform deploys the software on an external server, either for a single customer or for multiple firms (multi-tenant).

Maturity phase: Mature. EHS software has matured into a well-established market, with risk professionals leveraging it to manage operational safety, environmental compliance and incident reporting. Cloud-hosted solutions are now considered the baseline, with all 23 vendors in the most recent Verdantix Green Quadrant for EHS software offering this as standard (see [Verdantix Green Quadrant: EHS Software 2025](#)). Widespread adoption has been supported by the growing popularity of Software as a Service (SaaS) platforms, which lower IT infrastructure costs and improve accessibility across devices – benefitting risk teams looking for consistent, real-time visibility into EHS performance. Vendors such as Intellex, Sphera and TenForce continue to refine their web-based platforms to meet user demands. However, while EHS software remains a vital tool within risk functions – especially in high-hazard industries – many risk professionals are increasingly turning to broader enterprise risk management (ERM), ESG, and governance, risk and compliance (GRC) platforms that offer a more comprehensive view of organizational risk. Vendors are responding in turn, with SafetyCulture, for example, advancing its integration with wider risk functions across its unified platform. The overall shift suggests that while EHS software is mature and trusted, its role is becoming more specialized within the wider risk technology ecosystem.

Business value: Medium. Cloud-based EHS software delivers moderate business value to risk professionals by improving operational efficiency and enabling more consistent data capture across environmental, health and safety processes. Its SaaS deployment model supports faster implementation, regular updates and easier integration with existing risk management systems, reducing the burden on IT resources. For risk teams, this means improved visibility into compliance-related data and incident trends, aiding with proactive risk identification. However, its value remains 'medium', because EHS systems are typically treated as integrations into broader enterprise risk platforms, limiting their use in strategic and holistic risk analysis as a standalone tool. While cloud deployment enhances accessibility and scalability – especially for small and medium-sized enterprises (SMEs) – the insights generated are typically operational, rather than enterprise-level, making this a useful but not central tool for most risk professionals.

Pace of innovation: 10+ years. The EHS software market is experiencing a wave of innovation as vendors seek to differentiate themselves from competitors. We therefore do not expect this technology to reach the Decline stage within the foreseeable future. Some firms are exploring partnerships with edge technology providers: witness Intellex, which is incorporating wearable tech into its software offerings. On the customer side, the advantages of SaaS-based EHS solutions are becoming increasingly clear. Despite this, data security and safety remain key concerns, especially in multi-tenant cloud environments. To gain broader adoption – particularly in industries that are highly regulated or sensitive to data risks – vendors will need to strengthen their security measures and address these challenges head-on.

Example vendors: Alcumus, Benchmark Gensuite, BlueKanGo, ComplianceQuest, CONFORMiT, Cority, DNV, EcoOnline, Enhesa, Enterprise Health, ETQ, Evotix, GOARC, HSI (Donesafe), Ideagen (DevonWay), Ideagen (EHS), Intellex, INX Software, IsoMetrix, KPA, Origami Risk, Previsis, Pro-Sapien, Quentic, SafetyCulture, SafetyStratus, SAI360, SAP, Simple But Needed, SMS360, Sphera, StarTex Software, TenForce, UL Solutions, VelocityEHS, VisiumKMS, Xybion.



Business continuity and disaster recovery solutions

Definition: Business continuity and disaster recovery (BC/DR) software refers to digital tools and platforms that help organizations plan for, respond to and recover from disruptive events, such as cyber attacks, natural disasters and system failures. These solutions support the development of business continuity plans, automate incident response workflows and ensure that critical systems and data can be restored quickly, to minimize downtime. While business continuity focuses on maintaining operations during a disruption, disaster recovery centres on restoring IT infrastructure and data after the event.

Maturity phase: Mature. BC/DR software is a mature segment, with core capabilities such as back-up, recovery planning and continuity workflows well-established across industries. However, the market is undergoing a shift as many vendors evolve to become part of the faster-growing operational resilience segment. Driven by increasing regulatory pressure – most notably from the EU's Digital Operational Resilience Act (DORA) and the UK's Financial Conduct Authority (FCA) operational resilience rules – firms are expanding their expectations for end-to-end resilience beyond traditional BC/DR tools, towards integrated solutions that combine risk management, crisis response, third-party oversight and business continuity in a single platform.

Business value: High. BC/DR software provides significant business value by enabling organizations to swiftly recover from unexpected disruptions, thereby safeguarding revenue, maintaining customer trust and ensuring compliance. The financial impact of downtime is substantial: a [study by WTW](#) indicated that just 8% of firms believe that they have complete control over their supply chain risks, while 63% reported losses in 2024 and 2025 that were higher than expected. This explains why board-level interest in business continuity is returning to centre stage, with the proliferation of global risks pushing the C-Suite away from purely reactive methods of risk management, towards a focus on operational capacity during crises.

Pace of innovation: 10+ years. The pace of innovation for BC/DR software is expected to span a horizon of 10 years or more before approaching Decline, due to the complexity, criticality and regulatory sensitivity of the solutions involved. While core capabilities such as recovery planning, back-up automation and continuity workflows are now widely established, the segment is undergoing a new wave of innovation, driven by increased climate-related disruptions, cyber threats, hybrid IT environments and rising stakeholder needs around resilience. Emerging features such as real-time risk monitoring, AI-driven scenario modelling and automated orchestration also reflect a growing focus on preparedness and adaptability. The next phase of innovation will be increasingly tied to convergence with operational resilience and integrated risk management, with BC/DR serving as foundational components within a broader resilience ecosystem.

Example vendors: Archer, Everbridge, Fusion Risk Management, MetricStream, Mitrastech (Preparis), Premium Continuum (ParaSolution), Quantivate, Riskconnect (Castellan).

Claims management software

Definition: Claims management software (CMS) is designed to streamline and automate the end-to-end process of handling insurance, legal or warranty claims. CMS provides organizations with tools to efficiently record, process, track and settle claims, while ensuring regulatory compliance, accuracy and transparency.

Maturity phase: Mature. CMS is considered a mature market, because of its widespread adoption, established functionality and the presence of longstanding vendors with proven track records. Most large insurance, healthcare and legal organizations have already integrated digital claims systems into their core operations, where they are a standard part of the enterprise tech stack. The software's core features – such as automated workflows, document management, fraud detection, and integration with customer relationship management (CRM) and enterprise resource planning (ERP) systems – have become largely standardized across providers. Meanwhile, the industry has moved beyond basic digitization to focus on efficiency, compliance and analytics, reflecting a shift from early adoption to optimization. High regulatory scrutiny and the need for transparent, auditable claims processes have further driven adoption.

Business value: Medium. CMS has held its significance in the market by establishing and maintaining efficiency gains and cost reductions via automated insights, with the continuous arrival of increasingly unstructured data in the information chain pushing firms away from manual processes. [Milliman notes](#) that in many property and casualty lines, the top 10% of claims represent over 80% of all claims costs: a growing need to streamline higher-cost claims early in the claims management process is promoting growth in CMS solutions. Meanwhile, the insurance industry has experienced a significant rise in claims volumes. The [Association of British Insurers \(ABI\) reported](#) that in 2025 home insurance claims totalled £6.1 billion, while those caused by adverse weather accounted for £1.2 billion – a 14% increase from 2024. CMS solutions present an answer to this challenge, as the industry seeks not only the faster validation of claims, but wider operational bandwidth.

Pace of innovation: 10+ years. Contemporary CMS first emerged in the early 2000s. In 2026, the technology has shifted from basic claims processing to advanced analytics and predictive claims management. The pace of innovation has naturally slowed compared with that of emerging technologies, with the market having reached a state of maturity, enjoying standardized features and widespread adoption. Vendors are now focusing on incremental improvements such as enhanced analytics, better user experience and AI-assisted decision-making, rather than radical innovation. Nevertheless, CMS remains highly relevant and unlikely to enter a phase of Decline for at least the next decade. Its longevity will be driven by ongoing regulatory requirements, the growing complexity and volume of claims, and the foundational role the software plays in risk and legal processes.

Example vendors: A1 Tracker, Apex EDI, APP Tech, Appian, BriteCore, ClaimPilot, Duck Creek Technologies, DXC Technology, FileTrac Evolve, FINEOS, Guidewire, Insurity, LexisNexis, Majesco, Screenshot.



Business process mapping

Definition: Business process mapping is a digital tool that helps organizations visualize internal workflows and operations. It supports process standardization, identifies inefficiencies and risks, and serves as a foundation for automation, compliance and continuous improvement initiatives.

Maturity phase: Mature. Business process mapping software is in the Maturity phase of the technology life cycle. Its use has been widespread since the early 2000s, evolving from basic flowcharting tools such as Microsoft Visio to more sophisticated platforms such as Bizagi, Nintex and Signavio that support real-time collaboration, process simulation and integration with automation and enterprise resource planning (ERP) systems. Initially adopted by operations and process improvement teams, its value has expanded to risk, audit and compliance functions, where it supports control design and internal audits. While its core functionality – visualizing and analysing workflows – is now standardized, demand remains steady, due to the ongoing need for process transparency, efficiency and risk mitigation.

Business value: Low. Business process mapping software delivers low business value within the broader landscape of risk management technologies. It lacks the immediate impact of tools such as cyber threat detection or business continuity platforms, but continues to play a foundational role in understanding and mitigating operational risks. By providing clear visibility into how processes flow, where controls exist – or are missing – and the responsibility of stakeholders, it enables better risk identification, control design and audit readiness. It is especially useful for functions such as internal audit, compliance and operational risk, where understanding processes is critical to assessing exposure. However, because it is not inherently a real-time or dynamic risk response tool, its value is more enabling than strategic.

Pace of innovation: 5-10 years. Business process mapping software is likely to remain in the Maturity phase for another five to 10 years, before entering Decline. Its foundational role in operational risk, compliance and process improvement ensures its ongoing relevance, particularly in larger enterprises. While innovation has slowed, steady demand is sustained by integration with automation tools, governance, risk and compliance (GRC) applications and digital transformation initiatives. Over time, its standalone use may decline as process mapping becomes embedded within broader platforms such as ERP, workflow automation or integrated risk solutions.

Example vendors: Bizagi, ClickUp, Creately, Decisions, IBM (Blueworks Live), iGrafx Process360 Live, Lucidchart, Microsoft (Visio), Miro, Nintex, Pipefy, SAP (Signavio), Whale.



Data loss prevention solutions

Definition: Data loss prevention (DLP) technology encompasses solutions that provide visibility into data usage and movement, to address data-related threats, such as inadvertent or accidental data loss and sensitive data exposure. Critically, DLP works to enforce security policies for data at all stages, whether in use, in motion or at rest. This enables it to address data-related threats using remediation or warning features such as monitoring, alerting, quarantining and blocking suspicious or harmful activity.

Maturity phase: Mature. DLP technology entered the market in the early 2000s, focusing on unauthorized access prevention for sensitive data such as personally identifiable information (PII) and financial information. At the time, firms such as Verdasys (now Digital Guardian) were pioneers in offering DLP solutions that incorporated elements such as encryption, access controls and the monitoring of sensitive data. More recently, the widespread adoption of cloud and Software as a Service (SaaS)-based services have made firms more vulnerable to data loss due to weaker security barriers, creating demand for cloud-based DLP solutions. Vendors such as Digital Guardian and Symantec now offer targeted cloud DLP solutions for an added level of security, to protect cloud-stored data.

Business value: High. The emergence of highly sophisticated threats, such as ransomware, malware and phishing, in recent years has expanded the DLP technology threat landscape significantly. To adapt, vendors such as Endpoint Protector have introduced multi-operating system (OS) endpoint security across all possible data loss endpoints, while ServiceNow has launched a Digital Resilience Third-Party Information Register app, through which differing vendor data fields can be maintained and exported cleanly.

Pace of innovation: 10+ years. DLP solutions will continue to retain demand from firms in data-sensitive industries – spanning governmental organizations to financial and healthcare institutions – as they seek to become more proactive in the face of financial, reputational and operational threats. Vendors are leveraging AI and machine learning (ML) to enable them to better target sophisticated attacks, keeping pace with the evolving threat landscape. They are also innovating in other areas. Fortra, for example, provides email data loss prevention solutions to detect malicious or sensitive content buried within files. With customer demand set to grow as threats expand, DLP technology will see further innovation over the coming years.

Example vendors: Check Point, Cisco, Digital Guardian, Egress, Endpoint Protector (by CoSoSys), Fidelis Cybersecurity, Forcepoint, Fortra, McAfee, Micro, Netskope, Proofpoint, Safetica, ServiceNow, Symantec, Teramind, Trend.

Financial risk management software

Definition: Financial risk management software enables firms to identify, assess and continually monitor financial risks that can impact a firm's operations or profitability. Financial risk managers look for capabilities that target a range of issues, such as anti-money-laundering (AML) compliance, fraud detection and prevention, and credit scoring and assessments. The software is typically adopted by firms in high-risk data privacy industries, such as banking, insurance and healthcare.

Maturity phase: Mature. In addition to financial crises and market volatility over the past two decades, a string of regulations to protect customers and financial institutions has driven the adoption of financial risk management software, as firms seek to comply and mitigate risks. For example, in 2000 the UK introduced the Financial Services and Markets Act (FSMA) to protect consumers, maintain market confidence and create a framework for regulating the UK financial services industry. This was followed by the 2002 Proceeds of Crime Act, aimed at recovering losses from illicit activity, and the 2017 Money Laundering, Terrorist Financing and Transfer of Funds regulations, which set out a risk-based approach to customer due diligence (CDD). To help firms comply with these regulations and those abroad, ComplyAdvantage, an AML software provider, has offered fraud detection and transaction monitoring solutions since 2014. Recently, it introduced new AI-powered solutions. AML RightSource, another end-to-end AML software and financial crime advisor, offers compliance-aligned financial risk management software powered by AI.

Business value: High. According to [UK Finance](#), total cases of fraud rose by 17% between 2024 and 2025, with overall losses reaching £629.3 million – a 3% increase year on year. With rising fraud incidents, increasingly granular and more stringent financial regulations, and low barriers to entry, financial risk management software is highly valuable for businesses. By helping to mitigate potential financial threats in real time, and ensuring compliance with regulatory requirements, it reduces firms' exposure to losses and enables long-term financial stability.

Pace of innovation: 10+ years. Financial risk management software will continue to serve as a critical tool for managing financial risk portfolios, with cyber and deepfake AI threats on the rise. As more firms move towards proactive crisis strategies, AI-based financial risk management software is becoming critical to resilience, with vendors leveraging AI to enhance the accuracy and efficiency of their AML and fraud detection software (see [Verdantix The AI-Driven Revolutionization Of Fraud Risk Management In The Financial Sector](#)). Despite its maturity, the financial risk management software market will therefore continue to evolve and experience innovation over the next few years.

Example vendors: ACI Worldwide, Actico, AML RightSource, Arachnys, ComplyAdvantage, Featurespace, Feedzai, FICO TONBELLER, Nasdaq (Verafin), NICE Actimize, Oracle, SmartSearch, SymphonyAI, ThetaRay, Trulioo.



Whistleblower software

Definition: Whistleblower software enables employees and third parties to securely and anonymously report misconduct, ethical violations or compliance breaches. It typically incorporates case management, secure intake channels and audit trails, to support internal investigations and regulatory compliance.

Maturity phase: Mature. Whistleblower software is a mature and well-established segment within the broader ethics and compliance technology market. Over the past decade, driven by global regulations such as the US Sarbanes-Oxley Act and the EU Whistleblower Protection Directive, and increasing investor and employee expectations around transparency, adoption has become widespread across both the public and private sectors. Core functionality such as secure anonymous reporting, multilingual support and case management are now standard, with vendors focusing recent innovation on integration with governance, risk and compliance (GRC) systems, user experience and analytics that detect patterns in misconduct. The market has also seen consolidation, with firms such as EQS and NAVEX acquiring regional platforms to expand their reach. While the pace of innovation has slowed in recent years, whistleblower tools remain strategically important, especially as organizations link speak-up culture to risk prevention and ESG commitments.

Business value: Medium. Whistleblower software holds medium business value, but is more critical for organizations operating in regulated or high-risk sectors. The platforms provide a secure and structured way for employees and third parties to report misconduct, fraud or ethical breaches, surfacing issues before they escalate into costly legal or reputational crises. The importance of these tools is demonstrated by cases such as [Nestlé's 2025 CEO crisis](#), where complaints raised through the firm's Speak Up channel triggered an investigation, leadership upheaval and a significant crisis. As organizations place greater emphasis on integrity, transparency and culture, whistleblower software serves as a vital early warning system, helping to prevent risks that traditional controls may miss.

Pace of innovation: 5-10 years. Whistleblower software is expected to remain in the Maturity phase for another five to seven years, before entering Decline. Ongoing regulatory pressure is sustaining adoption, especially in less mature markets. While core features are now standardized, the tools continue to deliver strategic value by upholding a culture of transparency and supporting reputational risk management. Over time, the category is likely to be absorbed into broader GRC or ethics platforms; however, its relevance as a standalone solution will persist in the near term.

Example vendors: AllVoices, Aunetic, Case IQ, EQS (Got Ethics), EQS Integrity Line, Ethico, FaceUp, NAVEX, OneTrust, SpeakUp, Vault Platform, Valor.

Risk management technologies in Phase 5: Decline

Audit software

Definition: Audit software automates governmental and industry-specific compliance protocols. Through automation, it analyses compliance documents, integrates data storage, accesses trend analytics, tracks audit trails, links audit management, and plans future audits internally. Audit software usually presents all data in a single platform and generates feedback reports to prevent and correct issues in the auditing process. IT security measures are included in most audit software, but to varying degrees.

Maturity phase: Decline. Audit software is no longer able to command its own space within the market, mainly due to other, more integrated programmes offering holistic approaches to audit, compliance and risk management. Modern platforms in the space – provided by vendors such as NAVEX, Optro and Workiva – have focused on integrating audit measures into their wider GRC tools. Since its largest jump – between 2019 and 2020 – the audit software market has stagnated, while more up-to-date GRC tools that integrate audit measures are projected to grow to \$9.08 billion, at a CAGR of 11%, by 2029 (see [Verdantix Market Size And Forecast: Governance, Risk And Compliance Software 2023-2029 \(Global\)](#)). Audit software has therefore reached peak maturity and is now falling behind its GRC-contextualized successors; however, it is possible that its core function will re-emerge inside these models. Any standalone audit software will likely be driven by some form of continuous intelligence, as per the dominant market direction in 2026.

Business value: Medium. Audit software is a medium-value technology for many organizations, particularly as relevance wanes in the face of more integrated GRC platforms. While it continues to support essential functions such as audit planning and report development – given advancing regulatory requirements and increasingly granular reporting standards – its standalone nature limits its appeal in a business environment that now prioritizes connected, cross-functional systems. Audit software often lacks the scalability needed to grow alongside broader GRC needs, and its deployment is frequently hindered by high implementation costs, incompatibility with legacy infrastructure, and the need for user training. These factors make it an impractical option for many firms, which seek consolidated platforms that streamline compliance, risk and audit processes within a single interface.

Pace of innovation: 5-10 years. Few disruptive innovations have emerged in the audit software space in the last couple of years, with many firms investing in audit-infused GRC tools instead. Rather than introducing major new features, much of the recent innovation has focused on incrementally enhancing existing functionality – particularly around automation. Automated compliance support has emerged as a key driver of innovation in this area, streamlining regulatory reporting, automating routine checks and reducing manual effort in tracking compliance-related changes. More recently, AI-enabled technologies – particularly those using natural language processing (NLP) and machine learning (ML) – have advanced the field by enabling audit software to conduct continuous monitoring, rather than relying on periodic, snapshot-based reviews. The new systems can analyse large volumes of structured and unstructured data in real time, flag anomalies and identify financial risks as they emerge. This shift towards continuous auditing has the potential to make risk identification timelier and more proactive, although it remains a developing capability and is not yet standard across all solutions.

Example vendors: AuditFile, AuditPRO, CURA, Ideagen (Quality Management), Kroll (Resolver), MasterControl, NAVEX, Optro, Oversight Systems, Plan Brothers, SAI360, Workiva.

verdantix

Master the detail



reimagine the big picture

Verdantix is an independent analyst firm that supports a global client base through research, data and advisory.

Unlimited analyst inquiry service

The world's most influential businesses and forward-looking tech leaders rely on Verdantix to inform their critical decisions.

Verdantix analyst inquiries help you apply our research and data to your unique business context, so you can evaluate your market position, benchmark against competitors, sharpen your product and messaging, and navigate evolving market dynamics.

[Inquire now](#)

[Explore our research](#)

Contact

Verdantix Ltd,
Woolyard, 52-56 Bermondsey Street,
London SE1 3UD, United Kingdom

contact@verdantix.com
[@Verdantix](#)

