FAIR INSTITUTE

2026 State of Cyber Risk Management Report

From Compliance to Competitive Advantage:
The Quantified Value of Cybersecurity

2026 State of Cyber Risk Management Report Content 2

Executive Summary 3
Key 2025 vs. 2026 Comparative Call-outs 3
1. The Upward Surge in FAIR Adoption & CRQ Momentum 3
2. Pragmatic Calibration of Program Maturity 3
3. AI Evolves from Experimentation to Core Infrastructure 3
4. Closing the Boardroom Engagement Gap 4
5. Tooling and Infrastructure Re-alignment 4
6. From Cultural Hurdles to Structural Security Silos 4
2026 Core Takeaways 4
Our Research Methodology 5
The Evolution of Cyber Risk Management 6
CRM Programs Consolidate at High Maturity Levels. 7
The Correlation of Maturity 8
Cyber Risk Leaders Align Strategy with Financial and Proactive Outcomes 9
Cyber Risk Management Creates Value 11
Value Delivery through CRM Maturity 11
CRM Maturity Shifts Cybersecurity Posture 13
FAIR Success Leads to Better Outcomes 14
The Technology C-Suite Benefits the Most 15
CRM Is Integrated with Enterprise Risk 17
Organizations Tackle Third-Party Cyber Risk 18
The Strategic Landscape of Third-Party Risk 18
CRM Programs Automate as They Mature 20
CRM Automation Improves Business Outcomes 21
Programs Integrate with Non-Cyber Operations 23
Data Is the Lifeblood of Cyber Risk Management 25
AI Is Not Limited to Experimental Use 27
Challenges and Gaps Persist 29
The Future of Cyber Risk Management 31
Participants Demographics 32
About Our Sponsors and the FAIR Institute 37
GuidePoint Security 37
SAFE 37
The FAIR Institute 37

Executive Summary

Conducted in April 2026 by the FAIR Institute with sponsorship from **GuidePoint Security** and **SAFE**, the **2026 State of Cyber Risk Management** research examines how leading organizations are adapting their cyber risk programs to meet increasing business, regulatory, and operational demands. Based on a global survey of 400 cyber risk leaders and practitioners, the 2026 data reflects a maturing discipline that is transitioning from a siloed technical compliance function into a quantified, automated, and board-level strategic driver.

When contrasted with the 2025 findings, several critical macro shifts emerge that define the current state of the discipline:

Key 2025 vs. 2026 Comparative Call-outs

1. The Upward Surge in FAIR Adoption & CRQ Momentum

The framework's footprint as the global language for risk has expanded significantly. The percentage of businesses actively using or planning to use the FAIR model climbed from 46% in 2025 to 58% in 2026. This clear positive trend underscores that financial quantification is rapidly becoming the standard for expressing cyber risk in concrete business terms. Furthermore, organizations achieving high success with FAIR report a massive 52% success rate in driving actual enterprise risk reduction.

2. Pragmatic Calibration of Program Maturity

In 2025, respondents reported an exceptionally high maturity ceiling, with 0% claiming "Low Maturity" and 43% claiming "Very High Maturity". In 2026, a realistic recalibration has occurred. For the first time, 10% of organizations openly acknowledge "Low Maturity" as they consolidate programs , while the "Very High Maturity" segment normalized to 11%. The modern baseline for established capabilities has officially settled at "Moderate" to "High" maturity levels (78% combined).

3. AI Evolves from Experimentation to Core Infrastructure

The operational footprint of Artificial Intelligence has expanded dramatically. In 2025, only 48% of organizations utilized AI for isolated CRM capabilities. In 2026, AI engagement has surged to a combined 80%, with 37% actively deploying it and 43% experimenting. AI has transitioned into a foundational infrastructure for scale, serving as a powerful force multiplier that drives a highly proactive cybersecurity posture (71% of AI-integrated organizations describe their approach as proactive, compared to just 52% of non-AI users).

4. Closing the Boardroom Engagement Gap

A glaring gap highlighted in 2025 was that while boards universally approved risk thresholds, they actually used cyber risk data in less than half of participating organizations. Driven by the transition to expressing cyber risk in monetary terms (90% of quantitative practitioners now utilize financial framing), boardroom use has jumped significantly to 63% in 2026.

5. Tooling and Infrastructure Re-alignment

The technical landscape has shifted from specialized fragmentation back toward unified enterprise platforms. While the 2025 market saw a dominant 56% of organizations choosing special-purpose CRM tooling, 2026 data shows that 63% of programs now anchor their capabilities within core, general-purpose Governance, Risk & Compliance platforms. CRM software has stabilized at a strategic 23% segment to handle quantitative modeling and advanced workflow automation.

6. From Cultural Hurdles to Structural Security Silos

In 2025, the leading obstacles to cyber risk success were primarily cultural, led by stakeholder resistance and a lack of executive prioritization. In 2026, a sharp technical and structural barrier has risen to the top: "gaps between cybersecurity silos" (such as friction between CRM, vulnerability management, and threat teams) is now cited by 33% of organizations as a primary operational challenge.

2026 Core Takeaways

- **CRM is fueling business results:** Top outcomes include greater risk reduction (35%), improved team credibility (34%), and resources alignment with business priorities (32%).
- **High-maturity programs are proactive: 51%** of organizations rate their maturity as high (**40%**) or very high (**11%**). **62%** overall are proactive and report significantly higher success in board reporting and risk mitigation.
- **FAIR and CRQ momentum:** Adoption of FAIR or FAIR-aligned approaches continues to grow, with 58% of organizations either currently using (27%) or planning to adopt the framework (31%).
- **Executive decision-making:** Technology-focused C-suite leaders—CTOs (83%), CISOs (79%), and CROs (78%)—are the primary consumers of cyber risk information.
- **Automation and AI at scale:** 64% of organizations have mostly or fully automated CRM systems. AI adoption is widespread, with **80%** currently using (**37%**) or experimenting (**43%**), viewing it as a foundational enabler to scale CRM.
- **Board engagement is standard:** 97% of organizations have defined risk appetite levels, with **89% approved at the board level.**
- **Challenges remain:** With "gaps between cybersecurity silos" (33%) and "poor communication between departments" (46%) identified as leading obstacles.

Our Research Methodology

The **2026 State of Cyber Risk Management** study was designed to explore how organizations with established cyber risk management (CRM) programs are evolving their practices, adopting new technologies, and aligning with business priorities. The research was developed and fielded by the **FAIR Institute** in collaboration with **Hanover Research**.

The study focused exclusively on professionals directly involved in CRM execution to ensure high-quality, actionable insights. To achieve this, a rigorous multi-step qualification process was employed:

- **Survey Administration & Sample Size:** The survey was administered online in April 2026 using a recruitment panel. Following data cleaning and quality control, the final analysis includes a total of **400 qualified respondents**.
- **Target Audience & Geography:** Respondents were required to be age 22+ and work full-time in one of **14 target countries**. This global sample included major representations from the United States (38%), the United Kingdom (23%), Germany (6%), and France (6%).
- **Organization Size:** Participants were limited to those working at organizations with **1,000 or more full-time employees**. Nearly half (49%) of the organizations represented reported an annual revenue of **$5 billion or more**.
- **Professional Qualifications:** Respondents were required to work at an analyst level or above within specific departments, including Cybersecurity, Cyber Risk Management, Enterprise Risk Management, or Compliance.
- **Executive Alignment:** Every participant operates within the office of a key technology or risk executive, such as the **CISO (35%)**, **CRO (38%)**, **CTO (21%)**, or **CIO (5%)**.
- **Decision-Making Authority:** Participants were required to be involved in the decision-making process for the purchase of technology solutions at their company.
- **Knowledge Screener:** To ensure meaningful insights from practitioners, respondents who reported having "no cyber risk management capabilities" were disqualified. Additionally, all participants were required to pass a knowledge screener correctly identifying the primary purpose of a cyber risk assessment as "evaluating the potential likelihood and impact of cyber-related losses".

By design, this methodology ensures that the results reflect the perspectives of organizations that are actively managing cyber risk and leading the discipline forward.

The Evolution of Cyber Risk Management

Cyber risk management (CRM) has undergone a fundamental transformation from a niche technical concern to a formalized, board-level discipline. Historically, CRM was rarely captured in industry literature, but it has since been codified into numerous global standards and regulatory frameworks, including **ISO/IEC 27005**, the **NIST Cybersecurity Framework**, and the **EU Digital Operational Resilience Act (DORA)**. Today, CRM is increasingly regarded as a legal element of "due care" under prevailing case law in many jurisdictions.

The evolution is characterized by several key shifts in how organizations perceive and manage uncertainty:

- **From Qualitative to Quantitative:** Organizations are moving away from traditionally static "High/Medium/Low" qualitative labels toward continuous, business-aligned programs featuring **Cyber Risk Quantification (CRQ)**.
- **Financial Framing of Risk:** A defining trend in 2026 is the transition to expressing cyber risk in monetary terms. Among organizations utilizing fully quantitative approaches, **90%** now express risk in financial terms (e.g., dollars or euros).
- **Operational Integration:** CRM is no longer a siloed activity; it is being embedded into core IT and business functions, such as **IT Asset Management (90%)**, **Enterprise Risk Management (81%)**, and **Finance and Accounting (70%)**.
- **Technological Acceleration:** The discipline has evolved to embrace **automation (64%)** and **Artificial Intelligence (80% using or experimenting)** to manage risk at the pace of modern digital business.
- **Outcome-Oriented Strategy:** Modern CRM focuses on delivering cost-effective risk reduction rather than simple compliance. This shift allows cybersecurity leaders to justify budgets based on measurable impact, such as **improving loss prediction accuracy (34%)** and **enhancing decision-making with measurable metrics (31%)**.

As executive leadership and corporate boards demand greater transparency, the ability to translate technical vulnerabilities into probable loss event scenarios and magnitudes has become the hallmark of a mature CRM program.

CRM Programs Consolidate at High Maturity Levels

The 2026 study confirms that for organizations with established capabilities, the baseline for "moderate" maturity has become the industry floor. The distribution of maturity among the 400 respondents is as follows:

Survey Question: How mature would you rate your organization's cyber risk management capabilities overall?

Maturity Level	% of Total
Low maturity (i.e., we are in the early stages of our program or have not matured much from our starting point)	10%
Moderate maturity (i.e., we have a regular cadence for CRM processes and are regularly delivering value to our department or company)	38%
High maturity (i.e., we have a regular cadence for CRM processes, have developed advanced reporting and analytics, and are delivering significant value to our department and our company)	40%
Very high maturity (i.e., our CRM program is an integral part of how we plan, operate and transform our company's technologies)	11%

The Correlation of Maturity

In 2026, maturity is not a standalone metric but a primary indicator of operational success across several domains:

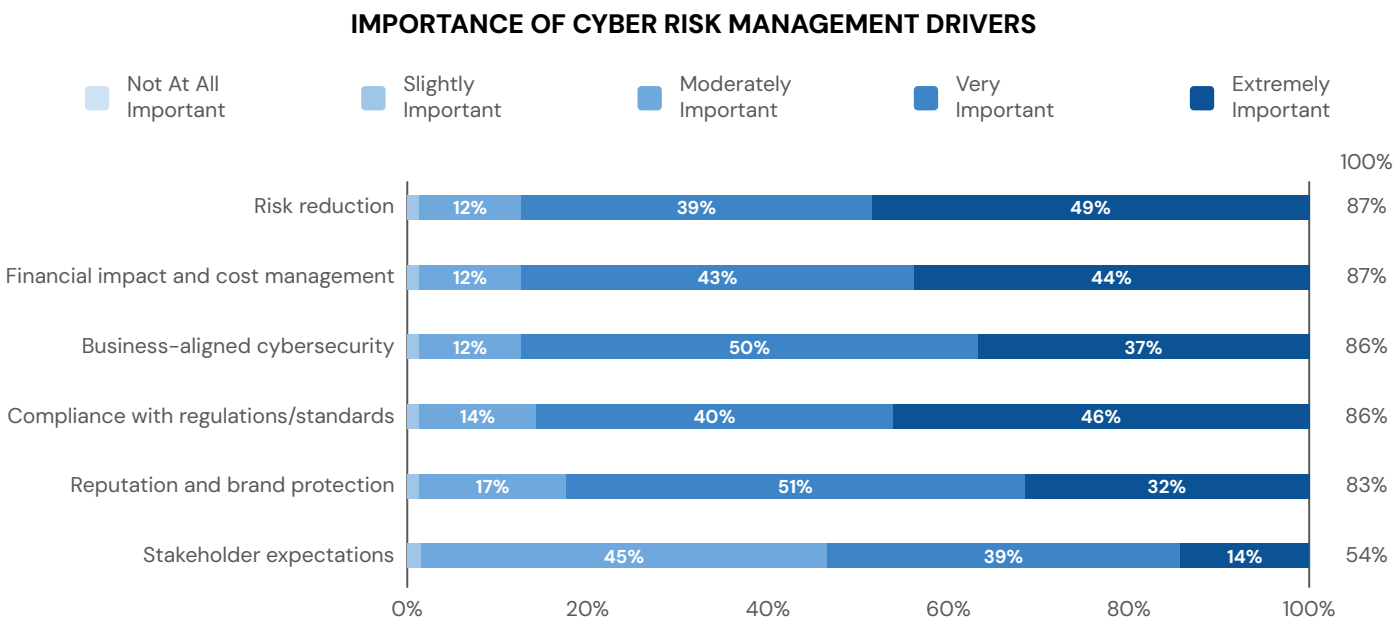
- **Proactive Posture:** 62% of organizations overall describe their cybersecurity efforts as proactive rather than reactive, a sentiment driven primarily by high and very-high-maturity teams.
- **Capability Strength:** Maturity is most pronounced in specific functional areas, including **Cyber Risk Mitigation (79%)**, **Cyber Insurance Coverage (74%)**, and **Cyber Risk Escalation (72%)**.
- **Resource Confidence:** High maturity correlates with resource stability; 46% of organizations strongly agree they have appropriate funding, and 49% are confident in their available skillsets.
- **Governance Effectiveness:** While maturity is high, effectiveness in governance remains a challenge. Only 35% of organizations—even among those with high maturity—describe their formal governance groups as "fully effective".

This data suggests that while the "mechanics" of CRM (processes and reporting) are reaching a state of high maturity, the "outcomes" (governance and cross-departmental integration) still represent the next frontier for growth.

Cyber Risk Leaders Align Strategy with Financial and Proactive Outcomes

In 2026, cyber risk management has moved beyond its technical origins to become a core strategic discipline. Organizations are increasingly tying cybersecurity efforts directly to enterprise-wide priorities, a shift reflected in both the strategic drivers they prioritize and their overall operational posture.

Survey Question: How important are the following drivers of cyber risk management at your organization?



Key 2025 vs. 2026 Comparative Call-outs

- **The Shift to Proactive Posture:** A significant 62% of organizations now describe their cybersecurity efforts as proactive rather than reactive. This shift indicates that leaders are increasingly using risk analysis to anticipate threats and mitigate vulnerabilities before they manifest as incidents.

- **Financial Framing of Risk:** Among organizations utilizing fully quantitative measures, 90% now express cyber risk in financial terms (e.g., dollars or euros). This financial translation allows leaders to move away from technical jargon and communicate with boards and executives in a language that informs capital allocation and business strategy.
- **Board-Sanctioned Boundaries:** Stakeholder alignment is reinforced at the highest levels, with 97% of organizations having defined risk appetite and tolerance levels, 89% of which have been formally approved by the board.
- **Resource Allocation:** Budgeting reflects this business alignment, with resources allocated based on asset criticality (50%), high-risk area prioritization (47%), and the potential impact of security breaches (43%).

By grounding decisions in business outcomes, cyber risk leaders are moving beyond traditional compliance checklists to gain a strategic advantage. This alignment ensures that cybersecurity is seen not as a "cost center," but as a critical enabler of digital growth and corporate reputation.

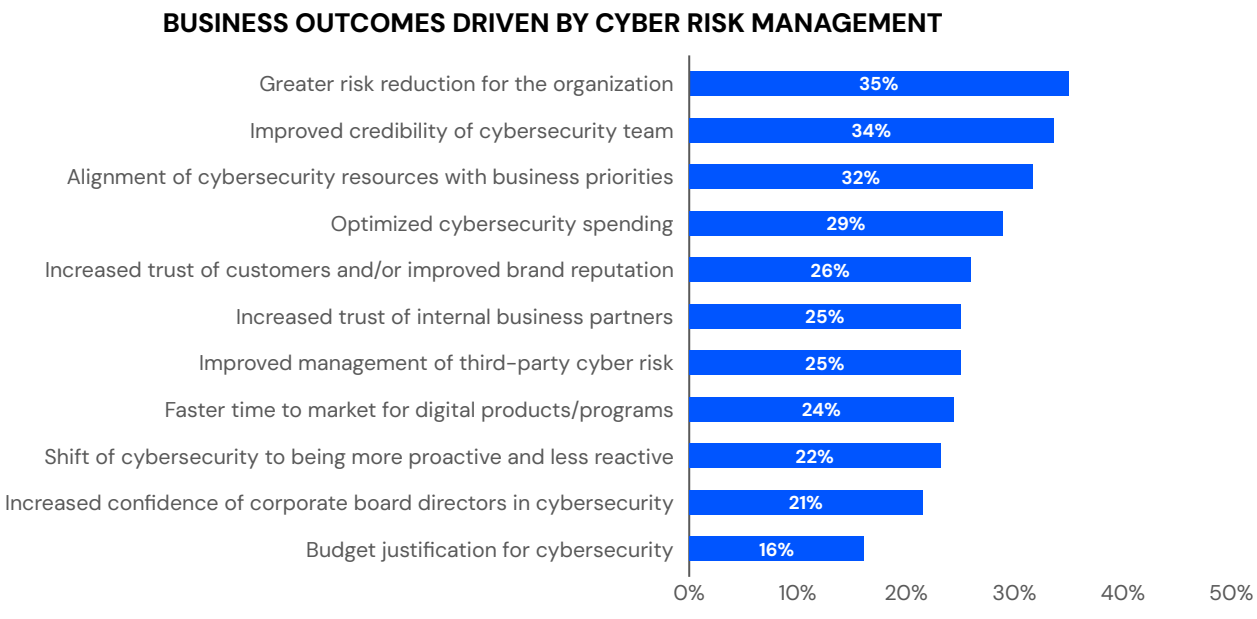
Cyber Risk Management Creates Value

In 2026, CRM has evolved into a strategic engine delivering clear business value across the enterprise. Rather than operating as a siloed technical function, CRM helps organizations achieve outcomes that align directly with enterprise goals of risk reduction, strategic alignment, and budget optimization.

Value Delivery Through CRM Maturity

The research confirms that while even moderate maturity delivers outcomes, the value scales significantly as programs advance. Organizations reporting higher CRM maturity are more likely to achieve top-tier business outcomes such as optimized spending and improved cybersecurity team credibility.

Survey Question: What business outcomes has cyber risk management been most helpful in driving at your organization? Select up to three (3)



The research highlights several key dimensions where CRM drives tangible organizational impact:

- **Enhanced Cybersecurity Credibility:** 34% of respondents report that CRM has improved the credibility of the cybersecurity team, transforming them into trusted advisors to the business.
- **Business Alignment:** 32% of organizations use CRM insights to ensure cybersecurity resources are aligned with actual business priorities.
- **Financial Optimization:** CRM supports data-driven financial decisions, with 29% of organizations using it to optimize cybersecurity spending and 16% leveraging it for budget justification.
- **External and Internal Trust:** The discipline fosters trust, with 26% of leaders reporting increased customer trust and improved brand reputation, while 25% note strengthened trust with internal business partners.
- **Operational Agility:** CRM contributes to faster time-to-market for digital products (24%) and shifts the cybersecurity posture from reactive to proactive (22%).

The data further demonstrates that **CRM maturity directly scales value**. Organizations reporting higher maturity levels are more likely to see these top-tier outcomes—such as optimized spending and risk reduction—compared to those with lower maturity ratings. By providing a clear, often financially quantified view of risk, CRM enables boards and executives to navigate uncertainty with confidence, turning cybersecurity from a cost center into a resilient competitive advantage.

CRM Maturity Shifts Cybersecurity Posture

In 2026, maturity is the primary driver of an organization's ability to transition from a defensive, reactive mentality to a strategic, proactive stance. The data reveals a direct correlation between advanced CRM capabilities and the effectiveness of an organization's cybersecurity posture.

Survey Question: Are your organization's cybersecurity efforts more proactive or reactive? [Segmented by CRM maturity level]

- **Proactive vs. Reactive Balance:** A significant **62%** of organizations now describe their cybersecurity efforts as proactive. Higher maturity organizations (Very High) are **91%** proactive , compared to only **37%** of moderate maturity organizations.
- **Strength in Mitigation:** Maturity is most pronounced in **cyber risk mitigation**, where **79%** of organizations report high or very high maturity.
- **Transfer and Escalation:** Organizations show strong maturity in **cyber insurance coverage (74%)** and **risk escalation (72%)**, indicating a sophisticated approach to risk treatment beyond purely technical controls.
- **Reporting and Disclosure:** Maturity in **board reporting (71%)** and **risk disclosure (65%)** suggests that programs are better at maintaining the transparency required by modern regulatory environments.
- **Operational Readiness:** Most organizations (**85%**) report strong effectiveness in their **risk treatment (response) processes**, showing that mature frameworks lead to more reliable execution.
- **Decision-Making Impact: 76%** of organizations are effective at **translating risk assessments into business decisions**, demonstrating that maturity shifts CRM from a compliance exercise to a decision-support tool.

As CRM capabilities grow through better data, automation, and decision support, the ability to manage cyber risk evolves into a dynamic business challenge rather than a static compliance issue. Organizations that lead in maturity are not just "more secure"; they are more agile, supporting smarter decisions that balance protection with business growth.

FAIR Success Leads to Better Outcomes

FAIR (Factor Analysis of Information Risk) has solidified its position as the industry standard for cyber risk quantification. Awareness is near-universal, and 2026 data shows that **58%** of organizations are either currently using FAIR (27%) or planning to adopt it within the next cycle (31%).

Survey Question: What business outcomes has cyber risk management been most helpful in driving at your organization? [Segmented by CRQ approach / success]

Top 3 Business Outcome	All Respondents	Very Successful with FAIR
Greater risk reduction for the organization	**35%**	**52%**
Improved credibility of cybersecurity team	**34%**	**29%**
Optimized cybersecurity spending / budget justification	**29%**	**29%**

The 2026 findings suggest that financial quantification alone is not the "silver bullet"; rather, it is the **successful implementation** of the FAIR methodology that allows organizations to bridge the gap between technical security findings and business-relevant risk management. This success leads to a more defensible cybersecurity strategy and optimized spending that aligns with the organization's overall risk tolerance.

The Technology C-Suite Benefits the Most

One of the clearest signs of CRM's evolution in 2026 is its direct support for executive and board-level decision-making. As accountability for enterprise risk management becomes more centralized, technology-focused leaders have emerged as the primary beneficiaries of risk-informed insights.

Survey Question: What roles/offices at your organization are using risk information? Select all that apply.

Offices/Roles Using Cyber Risk Information	% of Total
Chief Technology Officer (CTO)	83%
Chief Information Security Officer (CISO)	79%
Chief Risk Officer (CRO)	78%
Chief Information Officer (CIO)	74%
Chief Financial Officer (CFO)	71%
Chief Executive Officer (CEO)	65%
Board of Directors	63%
Business Unit and/or Product Leaders	14%

- **Primary Consumers of Risk Info:** Risk information is most heavily utilized in the offices of the **CTO (83%)**, **CISO (79%)**, and **CRO (78%)**.
- **Wider Executive Adoption:** Use of risk insights extends to the **CIO (74%)**, **CFO (71%)**, and **CEO (65%)**, indicating that CRM is increasingly serving as a strategic tool for the entire executive leadership team.
- **Board-Level Integration:** The Board of Directors uses risk information in **63%** of organizations, supported by the fact that **89%** of boards have formally approved defined risk appetite and tolerance levels.

- **Addressing the Line-of-Business Gap:** Despite high executive usage, only **14%** of business unit and product leaders currently engage with risk information. This highlights a significant opportunity to further embed CRM outputs into day-to-day operational decisions.
- **Quantification as a Bridge:** The shift toward financial quantification (utilized by **90%** of quantitative practitioners) has been essential in translating technical vulnerabilities into meaningful business terms for non-technical executives and board members.

The alignment between CRM and technology executive decision-making not only strengthens oversight but enables organizations to operate within clearly articulated, board-sanctioned risk boundaries. By narrowing the gap between senior leadership and business unit execution, organizations can achieve a more holistic and resilient risk posture

CRM Is Integrated with Enterprise Risk

The trajectory of 2026 data shows that organizations are moving away from treating cyber risk as an isolated IT problem and are instead embedding it into the core of enterprise-wide risk analysis and governance.

Survey Question: What best describes how cyber risks are integrated into enterprise risk management at your organization?

Integration of Cyber Risks with Enterprise Risk Management (ERM)	% of Total
Cyber risks are communicated to ERM and managed together with enterprise risks	53%
Cyber risks are communicated to ERM but managed separately	40%
Cyber risks are not communicated to ERM / No ERM function	<7%*

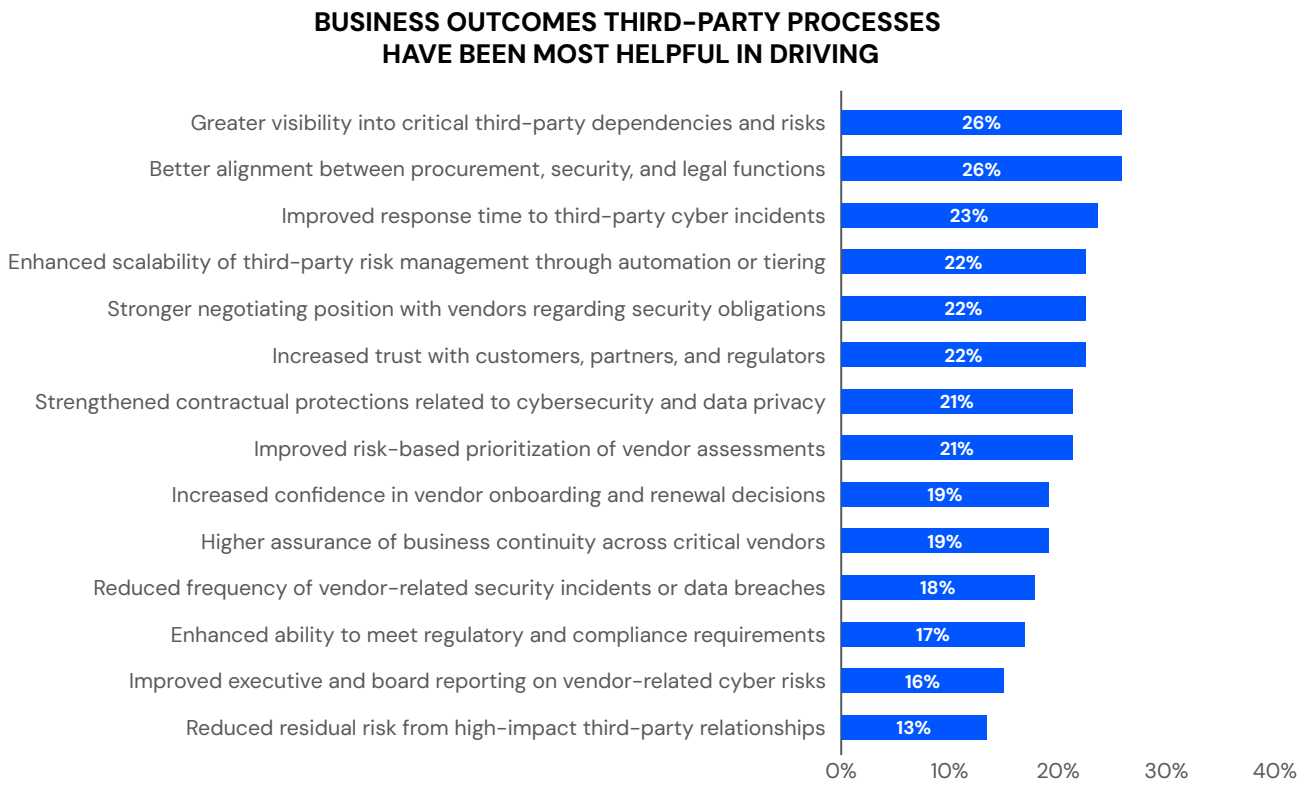
- **Unified Management:** More than half of organizations (**53%**) now report that cyber risks are communicated to enterprise risk management and managed together with other enterprise risks.
- **Shared Communication:** An additional **40%** of organizations communicate cyber risks to ERM but continue to manage them as a separate risk category.
- **Strategic Oversight:** This convergence ensures that cyber risk is evaluated alongside financial, operational, and reputational risks, facilitating more comprehensive board-level oversight.
- **Standard Alignment:** Leading organizations are increasingly aligning with standards like the **NIST IR 8286** series, which urges treated cyber risk as a fundamental component of enterprise reporting and governance.
- **High-Performing Hallmarks:** Tighter integration between CRM and ERM is quickly becoming a hallmark of high-performing organizations, as it fosters a shared risk language and clearer accountability for technology risks.

By integrating these functions, organizations can better prioritize cybersecurity investments based on their potential impact on the entire enterprise rather than just the IT department.

Organizations Tackle Third-Party Cyber Risk

As digital ecosystems become increasingly complex, third-party cyber risk has emerged as a strategic priority. The 2026 data confirms that managing these risks is now a nearly universal practice, with organizations applying varying degrees of rigor to their vendor relationships.

Survey Question: What business outcomes have your third-party cyber risk management processes been most helpful in driving at your organization?



The Strategic Landscape of Third-Party Risk

- **Universal Adoption:** 95% of organizations now apply cyber risk management processes to their third parties.

- **Management Rigor:** More than half of organizations (53%) strictly apply these processes, while 42% utilize a looser or more informal approach.
- **Measurement Practices:** Measurement remains mixed; 44% of organizations quantify third-party risk using a combination of both financial and non-financial methods.
- **Technology Foundations:** Execution is heavily anchored in technology, with 90% of organizations leveraging GRC platforms.
- **Tangible Business Value:** Third-party processes are driving visibility into dependencies (26%) and cross-functional alignment (26%).

While the discipline is widespread, a maturity gap persists: only 64% of respondents rate their third-party CRM as high or very high maturity, compared to the 62% who report similar maturity levels for their first-party programs. This suggests that while organizations have established the necessary infrastructure, the next phase of evolution will focus on increasing the rigor and quantitative accuracy of vendor risk assessments.

CRM Programs Automate as They Mature

In 2026, cyber risk management has moved beyond manual spreadsheets to become a tech-enabled discipline. The data indicates that automation is no longer an "add-on" but a foundational element that scales alongside program maturity.

Survey Question: Are your organization's current cyber risk management systems manual or automated?

Degree of CRM System Automation	% of Total
Mostly or fully automated	64%
Even mix of manual and automated	35%
Mostly or fully manual	<1%*

- **Broad Adoption of Automation:** Nearly two-thirds of organizations (**64%**) report that their cyber risk management systems are now mostly or fully automated.
- **The Hybrid Reality:** An additional **35%** of organizations utilize an mix of manual and automated systems, indicating a transition phase for many mid-maturity programs.
- **Correlation with Maturity:** Higher maturity levels are strongly associated with automation. For instance, while overall CRM maturity is rated High or Very High by 51% of respondents, these same organizations lead the charge in adopting automated workflows.
- **Shift to Specialized Tools:** While **63%** of organizations still anchor their programs in GRC platforms, there is a distinct move toward specialization; **23%** now utilize special-purpose CRM software to handle complex quantification and reporting tasks.
- **Efficiency Gains:** Automation is cited as a key driver for improving risk treatment processes, with **85%** of organizations reporting that their risk response processes are now highly effective due to these technological supports.

Automation helps CRM teams spend less time on data collection and more on analysis and strategic decisions. As programs mature, real-time data and automated reporting become critical for proactive cybersecurity.

CRM Automation Improves Business Outcomes

In 2026, automation is no longer just a luxury for large-scale operations; it has become a primary driver for achieving the essential business outcomes expected of a modern cyber risk management program. The data indicates a powerful correlation: as organizations automate their CRM systems, they see a direct improvement in their ability to reduce risk and align with the business.

Survey Question: What business outcomes [has CRM] | [have your third-party CRM processes] been most helpful in driving at your organization? (Segmented by degree of automation)

Business Outcome	Partial Automation	High Automation
Greater risk reduction	36%	41%
More optimized cybersecurity spending	32%	37%
Better alignment across security, legal, and procurement	18%	34%
Improved scalability in third-party risk management	14%	28%
Reduced residual risk from high-impact third parties	17%	26%

- **Enhanced Scalability and Speed:** 64% of organizations report that their CRM systems are mostly or fully automated, allowing them to process risk data at a pace that matches digital business operations.
- **Improved Risk Treatment:** Organizations with high levels of automation report strong effectiveness in their risk treatment and response processes (85%), as automated workflows reduce the time between detection and mitigation.
- **Data-Driven Budgeting:** Automation facilitates the use of quantitative risk assessments, which 34% of leaders say improves accuracy in predicting potential losses and 31% say enhances decision-making with measurable metrics.

- **Optimized Spending:** By automating the collection of asset and threat data, 29% of organizations have been able to better optimize their cybersecurity spending, ensuring resources are directed toward the highest-impact threats.
- **Specialized Software Adoption:** To drive these outcomes, 23% of organizations have moved toward special-purpose CRM software, which provides advanced quantification and workflow automation that traditional GRC tools may lack.

Ultimately, automation bridges the gap between raw data and executive action. Organizations that embrace automated CRM systems are not only more efficient but are also more successful at translating complex risk assessments into the clear business decisions required by senior leadership and corporate boards.

Programs Integrate with Non-Cyber Operations

In 2026, cyber risk management is no longer confined to security teams; it is increasingly embedded across the operational fabric of the enterprise. Data shows that organizations are integrating CRM into a diverse array of business and IT functions, reflecting its growing role in day-to-day decision-making and governance.

Survey Question: Within which operational processes or disciplines is cyber risk management integrated at your organization?

Operational Process or Discipline Integrated with CRM	% of Total
IT asset management/configuration management	90%
Enterprise risk management	81%
IT service management (e.g., ticketing, resolution)	79%
Finance and accounting	70%
Legal and compliance	64%
Vendor/supply management	55%
Supply chain management	34%
Product development/management	17%
Change management	16%
Human resources	10%

The patterns of integration reveal a discipline that is shifting from a siloed practice to a shared enterprise responsibility:

- **Technical Foundations:** Integration is most consistent within IT asset management/configuration management (90%), enterprise risk management (81%), and IT service management processes such as ticketing and resolution (79%).

- **Business Disciplines:** CRM has extended into core business functions, including finance and accounting (70%) and legal and compliance (64%).
- **Third-Party Alignment:** Over half of organizations (55%) have integrated CRM with vendor and supply management.
- **Emerging Integration Points:** Tighter collaboration is still developing in areas such as supply chain management (34%), product development and management (17%), change management (16%), and human resources (10%).

Despite opportunities for further improvement in areas like HR and product development, the trend is clear: CRM is becoming a standardized operational discipline. By embedding risk analysis into non-cyber operations, organizations ensure that technological risk is evaluated alongside the business changes that often introduce or alter those risks.

Data Is the Lifeblood of Cyber Risk Management

Cyber risk is fundamentally a problem of uncertainty, and effective CRM programs in 2026 reduce that uncertainty by grounding decisions in measurable inputs from a diverse range of telemetry and business data. The breadth of these data inputs reflects both the rising complexity of the threat landscape and the maturing state of risk practices.

Survey Question: What data does your organization regularly use for cyber risk management?

Data Sources Used for CRM	% of Respondents
SIEM data and/or network traffic logs	65%
Third-party risk assessments	63%
Incident response records	57%
Endpoint security data	57%
Cyber threat intelligence (CTI) data	54%
Compliance audit results	51%
Vulnerability assessment findings	46%
Vulnerability assessment reports	44%
Cloud management systems	40%
Asset data	38%
User access logs	21%
Penetration testing / red teaming results	21%
Loss data	16%
Product/service definitions	11%

- **Primary Technical Sources:** Analysis is heavily fueled by **SIEM data and network traffic logs (65%)**, providing real-time visibility into potential threat activity.

- **Third-Party Integration: Third-party risk assessments (63%)** are a critical feed, ensuring that external dependencies are factored into the enterprise risk profile.
- **Security Telemetry:** Organizations rely consistently on **endpoint security data (57%)** and **incident response records (57%)** to model probable loss scenarios.
- **Intelligence and Compliance:** Programs are supported by **cyber threat intelligence (CTI) data (54%)** and **compliance audit results (51%)** to align technical findings with regulatory expectations.
- **Infrastructure Visibility:** Data from **vulnerability assessment findings (46%)** and **cloud management systems (40%)** allow for a more accurate mapping of the attack surface.
- **Business Context:** While still emerging, the use of **asset data (38%)** and **loss data (16%)** helps programs communicate findings in business-relevant, financial terms.

The ability to operationalize this diverse telemetry allows CRM programs to better assess likelihoods, model potential financial impacts, and prioritize mitigation efforts based on actual evidence rather than intuition. In 2026, data-driven CRM is the baseline for organizations seeking a clearer and more defensible picture of their risk exposure.

AI Is Not Limited to Experimental Use

In 2026, Artificial Intelligence has officially transitioned from a promising emerging technology to a foundational infrastructure for Cyber Risk Management. The research confirms that AI is no longer a peripheral tool for experimentation but a pervasive enabler of scale, consistency, and proactive defense.

Survey Question: What is your organization's experience with using artificial intelligence (AI) for cyber risk management?

AI Usage Status	% of Total
Currently using AI	37%
Experimenting with AI	43%
Plan to adopt AI	20%

- **Widespread Adoption:** A combined **80%** of organizations are actively engaged with AI, with **37%** already utilizing it for core CRM functions and **43%** in the experimentation phase.
- **Imminent Expansion:** Of the organizations not yet fully using AI, **60%** expect to implement it within the next 12 months or sooner.
- **The Maturity Link:** AI adoption is strongly correlated with CRM maturity. Organizations using AI report significantly higher maturity across major capabilities, including board reporting, risk mitigation, and third-party risk management.
- **A Proactive Force Multiplier:** AI users demonstrate a far more proactive cybersecurity posture. **71%** of AI-integrated organizations describe their approach as proactive, compared to only **52%** of non-AI users.
- **Strategic Opportunity Areas:** Leaders see the most significant value in **automated risk quantification (42%)**, **workflow automation (40%)**, and **forecasting and scenario simulation (40%)**.

- **Operational Capabilities:** Beyond quantification, AI is being leveraged for threat detection, incident response, and processing unstructured data like vendor contracts and SOC2 reports to populate risk models.
- **Persistent Concerns:** Despite rapid adoption, implementation is tempered by **regulatory uncertainty (37%)**, **lack of mature AI-specific risk assessment models (32%)**, and concerns over **insider misuse or misconfiguration (30%)**.

As organizations face increasing internal demand for credible, data-driven decisions, AI is becoming the essential infrastructure required to navigate uncertainty at the pace of modern business.

Challenges and Gaps Persist

Even among organizations with established and maturing cyber risk management programs, significant human, organizational, and technical obstacles remain in 2026. While technical capabilities are advancing, the most persistent barriers are rooted in organizational friction and governance failures.

Survey Question: What challenges with cyber risk management does your organization face? Select all that apply.

CRM Challenge	% of Total
Gaps between cybersecurity silos	33%
Lack of reliable threat intelligence data	28%
Incompatible culture or mindset for CRM	23%
Lack of adequate data about third-party controls	21%
Resistance from peers/stakeholders	21%
Lack of executive commitment or prioritization	16%

- **Fragmentation and Silos:** The most frequently cited challenge is the existence of gaps between cybersecurity silos, such as those between CRM, vulnerability management, and threat management (33%).
- **Governance and Communication Failures:** Poor communication between departments is the single largest gap in governance and accountability structures, affecting 46% of organizations.
- **Cultural Resistance:** 23% of organizations struggle with an incompatible culture or mindset for cyber risk management.
- **Executive Commitment:** Despite formal board-level approvals, 16% of respondents still cite a lack of executive commitment or prioritization as a primary challenge.

- **Peer and Stakeholder Friction:** Resistance from peers and internal stakeholders remains a barrier for 21% of organizations.
- **Technical Data Gaps:** Organizations continue to face difficulties obtaining reliable threat intelligence data (28%) and adequate data regarding third-party controls (21%).
- **Resource and Staffing Confidence:** While funding and skill sets are viewed relatively positively, only 26% of organizations express strong confidence in their current staffing levels.
- **Ineffective Governance Groups:** Although formal governance groups are widespread, only 35% of organizations describe them as fully effective, with 12% stating they are not effective at all.
- **Training Gaps:** A lack of regular training and awareness programs is noted as a governance gap by 21% of respondents.

These findings suggest that as the technical "mechanics" of CRM—such as quantification and automation—reach maturity, the next frontier for leaders is solving the "human" element. Success in 2026 and beyond will depend on closing these communication gaps and fostering a risk-aware culture that transcends traditional departmental boundaries.

The Future of Cyber Risk Management

As of 2026, CRM has entered a new era defined by risk quantification, massive-scale automation, and business-centric impact. While CRM is mandated across many industries and countries, it is no longer constrained by simple compliance checkboxes; instead, it is maturing into a strategic discipline that empowers organizations to navigate uncertainty with confidence.

Several powerful trends are shaping the future outlook through 2029:

- **Internal Demand Will Surge:** Nearly **89%** of organizations expect demand for CRM to increase over the next three years, driven by rising executive awareness and the need for data-driven cybersecurity decisions.
- **FAIR as the Global Language:** With **58%** of organizations currently using or planning to adopt the FAIR model, financial quantification is rapidly becoming the standard for expressing cyber risk in business terms.
- **Institutionalization of AI:** What began as experimentation is quickly becoming core infrastructure. Most organizations are already using or experimenting with AI (80%), and these technologies are now foundational to effective, real-time CRM.
- **Board-Level Integration:** Cyber risk oversight is becoming permanently embedded into enterprise governance. **89%** of organizations already have board-level approval for risk appetite and tolerance levels, ensuring that security boundaries are set at the highest level of leadership.
- **Investment Growth:** To meet these evolving demands, **72%** of organizations plan to increase their investment in cyber risk management over the next 12 months.
- **Regulatory Accelerants:** Far from being a burden, regulatory developments are acting as a positive force; **83%** of organizations report that regulatory changes have had a positive impact on their current CRM strategy.

Together, these shifts point toward a future where cyber risk is managed not just to prevent losses, but to deliver strategic value. CRM is evolving into a proactive, data-driven discipline that protects what matters most in an increasingly digital world.

Participant Demographics

Age	% of Total
25 to 34	22%
35 to 44	49%
45 to 54	27%
55+	2%

Country	% of Total
United States	38%
United Kingdom	23%
Australia	9%
Canada	6%
France	6%
Germany	6%
Netherlands	4%
Sweden	3%
Belgium	2%
Norway	2%
Denmark	1%
Finland	1%
Luxembourg	<1%

Department / Job Function	% of Total
Information Technology	21%
Cybersecurity	18%
Information Security	17%
Cyber Risk Management	13%
Enterprise Risk Management	13%
Compliance	12%
Third-Party Risk Management	7%

Office	% of Total
Chief Risk Officer (CRO)	38%
Chief Information Security Officer (CISO)	35%
Chief Technology Officer (CTO)	21%
Chief Information Officer (CIO)	5%
Chief Financial Officer (CFO)	<1%
Internal Audit	<1%

Industry	% of Total
Manufacturing	17%
Retail	14%
Banking	11%
Financial Services	8%
Healthcare/Medical	8%
Construction/Architecture	6%
Insurance	6%
Information Technology	5%
Telecommunications	5%
Automotive	4%
Distribution/Transportation	3%
Consumer Products (CPG)	3%
Utilities	3%
Oil and Gas	3%
Education	2%
Hospitality/Travel	2%
Accommodation and Food Services	2%
Arts, Entertainment, and Recreation	1%

Organization Size	% of Total
1,000 to 4,999 employees	31%
5,000 to 24,999 employees	31%
25,000 to 49,999 employees	22%
50,000 employees or more	16%

Job Level	% of Total
Associate/Analyst	25%
Manager/Sr. Manager	25%
Director/Sr. Director	38%
Vice President/Sr. Vice President	10%
C-Suite Executive	3%

Decision-Maker Status	% of Total
Primary decision maker	6%
Shares decision-making authority	46%
Participates by giving input	49%

Years of Experience	% of Total
1 to 5 years	18%
6 to 10 years	28%
11 to 15 years	35%
16 to 20 years	15%
More than 20 years	4%

Annual Revenue	% of Total
$50,000,000 to $249,999,999	4%
$250,000,000 to $499,999,999	7%
$500,000,000 to $999,999,999	12%
$1,000,000,000 to $4,999,999,999	28%
$5,000,000,000 or more	49%

About Our Sponsors and the FAIR Institute

The FAIR Institute thanks GuidePoint Security and SAFE for their counsel and support for this Research.

GuidePoint Security

GuidePoint Security brings together proven expertise, great relationships, and leading technologies to solve our client's most complex cybersecurity challenges. As a trusted cybersecurity advisor and partner, GuidePoint keeps people, data, and operations safe. We deliver tailored cybersecurity services that adapt to safeguard the nation's leading organizations today and provide complete confidence in their cybersecurity tomorrow. Stronger Together. Protecting What's Next. Learn more at GuidePointSecurity.com

SAFE

SAFE is the leader in Autonomous Cyber Risk Management. The SAFE platform unifies solutions for AI Security Posture Management (AI-SPM), Continuous Threat Exposure Management (CTEM), Cyber Risk Quantification (CRQ), and Third-Party Risk Management (TPRM), enabling organizations to continuously assess, prioritize, and reduce cyber risk across the enterprise and AI ecosystem. Trusted by 10% of Fortune 500 companies including Apple, AT&T, and Delta Air Lines. SAFE has raised $170 million to redefine how cyber risk is managed in the age of AI. Learn more at www.safe.security.

The FAIR Institute

The FAIR Institute is a non-profit professional organization dedicated to advancing the discipline of measuring and managing cyber and operational risk. With over 19,000 members worldwide, the Institute is recognized as a leading authority on cyber risk quantification and best practices in management. The FAIR Cyber Risk Management Framework, based on the industry's leading CRQ methodology, has been adopted by organizations across sectors to enhance security governance and risk-informed decision-making. Learn more at www.fairinstitute.org.


FAIR
INSTITUTE