2025 Strategic Roadmap for Cyber GRC

4 October 2024 - ID G00816595 - 35 min read

By: Jie Zhang, Michael Kranawetter

Initiatives:Cyber Risk; Build and Optimize Cybersecurity Programs

Exposure to a range of new cyber-risk and compliance obligations is a growing issue for the cyber GRC practice. Security and risk management leaders can use this research to pivot from a reactive, compliance-focused approach to a proactive, further-automated one.

Overview

Key Findings

- The evolving regulatory landscape and expanding attack surfaces have made it challenging for organizations to align Cyber GRC with their overall risk management strategy, necessitating a strategic shift. However, many SRM leaders are struggling to adapt to these changes.
- The focus on meeting regulatory requirements often leads to a reactive approach to cyber-risk management and assessment. As a result, there is typically lower engagement and collaboration between the cybersecurity team and the business.
- Many Cyber GRC management processes lack sufficient and relevant technology automation, leading to resource drain and control testing fatigue.

Recommendations

- Establish and formalize the governance component of a Cyber GRC function by utilizing frameworks like the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0 or similar standards and frameworks. This can lead to an explicit boundary and connection between Cyber GRC and the overall risk management objectives.
- Combine compliance and risk management effectively by prioritizing the implementation of impact-based assessments and automated, continuous monitoring capabilities.
- Alleviate the resource burden on the SRM leader and elevate the maturity of the Cyber GRC function by implementing purpose-designed Cyber GRC tools with capabilities such as continuous control monitoring, embedded AI features, and cyber-risk quantification.

Strategic Planning Assumptions

By 2027, one-third of large organizations will have redesigned their cybersecurity control testing and risk assessment processes to alleviate the resource burden on their Cyber GRC functions by cutting time spent on auditing technical controls in half or more.

By 2028, 50% of organizations that have successfully implemented impact-based cyber-risk assessment across all cyber-risk categories will experience a significant improvement in risk prioritization and minimization of manual effort.

Introduction

Cyber governance, risk and compliance (cyber GRC) is a specialized strategic framework that integrates cybersecurity-specific tools, methodologies, processes and standards to align business operations with relevant security investments. This framework is designed to manage cyber risks and ensure regulatory compliance within the digital landscape. Governance involves defining decision rights, leadership, organizational structures and processes that ensure cybersecurity controls are effectively implemented and maintained. Risk management focuses on identifying, assessing, mitigating and reporting cyber risks, while compliance ensures that the organization meets all legal and policy requirements related to cybersecurity.

Many organizations have adopted a mix of various standards and best practices for cyber GRC, but often there are inconsistencies in the processes followed. There could be multiple risk registers used by different risk domains, but they are not at all or only partially connected. Security and risk management (SRM) leaders have ad hoc engagement and semiroutine collaboration with other risk domains and key GRC and business leaders outside cybersecurity. Various committees and subcommittees might be in place, but not fully effective.

The cyber GRC practice is often driven by a melange of mandates, typically driven by external compliance requirements and risk evaluations focused on IT assets. There are limited linkages and guidance between cyber GRC and the broader business objectives and risks. Various tools are used to support cyber GRC (including Excel spreadsheets), lacking a standardized and integrated toolset for managing and tracking cyber risks.

It is important for SRM leaders to evolve their cyber GRC practice to be more strategically focused for the following reasons:

- **New responsibility territory:** The expanding digital landscape has made it necessary for SRM leaders to take on a larger role in enterprise risk management (ERM). New regulations and framework updates are introduced regularly, and SRM leaders need to adapt cyber GRC strategies to address these changes effectively. In many organizations, SRM leaders are now responsible for not only the security and technology aspects, but also for integrating and enabling innovation into non-cyber-GRC aspects (such as IT GRC and corporate GRC) of their organizations. This shift in responsibility is crucial as it ensures that cybersecurity is integrated into the overall business strategy, aligning security investments with business goals. For example, the recent U.S. SEC rule on disclosure management for public companies, the updates in the NIS 2 EU directive and the introduction of NIST CSF 2.0 necessitate a proactive approach to cybersecurity and compliance. By evolving their cyber GRC focuses, SRM leaders can ensure that their organizations are prepared to mitigate relevant emerging risks and comply with evolving regulations.

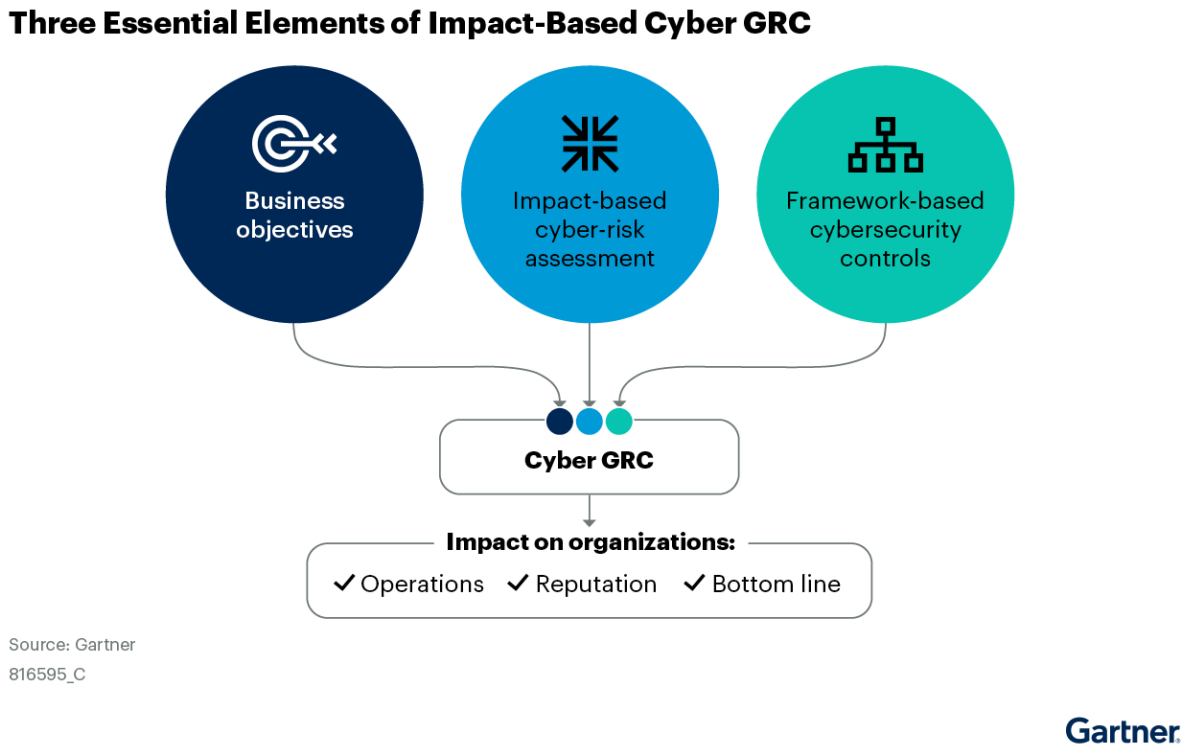
- **Trust of stakeholders:** SRM leaders need to address the concerns of stakeholders directly and within context, particularly those of boards of directors and C-suite executives. Ineffective communication, an increasing number of security incidents, missed digital business opportunities and limited demonstrable value can erode trust and satisfaction in the SRM leader's role and the performance of the cybersecurity management program. By strategically evolving their cyber GRC practice, SRM leaders can demonstrate their commitment to improving engagement, alignment, optimal allocation of resources, managing risks and assuring compliance. This can help rebuild trust and enhance the perception of the SRM leader's value within the organization.

- **Resource constraint:** This has been a significant challenge for SRM leaders and their teams. Reactive risk assessment, siloed control testing and project-based compliance efforts can strain limited resources, including budget, personnel and technology investments. By strategically aligning cyber GRC efforts with business priorities, the CFO's agenda, ERM, various compliance efforts and business risk profiles, SRM leaders can optimize resource allocation. This ensures that resources are allocated effectively to address the business perspective of most critical risks and compliance requirements. As a result, cost efficiency and resource utilization are improved, enabling SRM leaders to achieve more with limited resources.

- **Control mapping and framework integration:** SRM leaders must navigate a complex landscape of overlapping cybersecurity frameworks and standards, such as ISO/IEC 27001 and NIST CSF, to name the most dominant. Mapping controls to these various frameworks is essential for ensuring comprehensive coverage and avoiding redundant efforts. By strategically aligning cyber GRC practices, SRM leaders can streamline control implementation and assessment processes across multiple regulatory requirements. This approach not only simplifies compliance efforts, but also enhances the organization's overall security posture by ensuring that all critical areas are addressed. For example, leveraging a unified control framework can help in identifying commonalities and gaps, thereby optimizing resource allocation and reducing audit fatigue. This holistic view enables SRM leaders to demonstrate a robust and cohesive cybersecurity strategy, which is crucial for compliance and stakeholder confidence.

There are three essential elements that a strategic cyber GRC practice should have: business objectives, impact-based cyber-risk assessment and framework-based cybersecurity controls (see Figure 1). When these three elements are interconnected, it allows for a more deliberate and risk-based approach, where cybersecurity measures are tailored to address specific risks that could have the most significant impact on the organization's operations, reputation and bottom line (see How to Perform a Business Impact Analysis).

Figure 1: Three Essential Elements of Impact-Based Cyber GRC



Building an impact-based cyber GRC practice requires a set of inputs. For example, a clear, guided cyber-risk appetite originates from the business side or specific business owners of processes and data assets. This leads to accurate prioritization when SRM assigns resources for risk treatment. Equally, when the set of necessary inputs are available and continuously updated, an impact-based cyber GRC can deliver the proper outcomes (see Table 1).

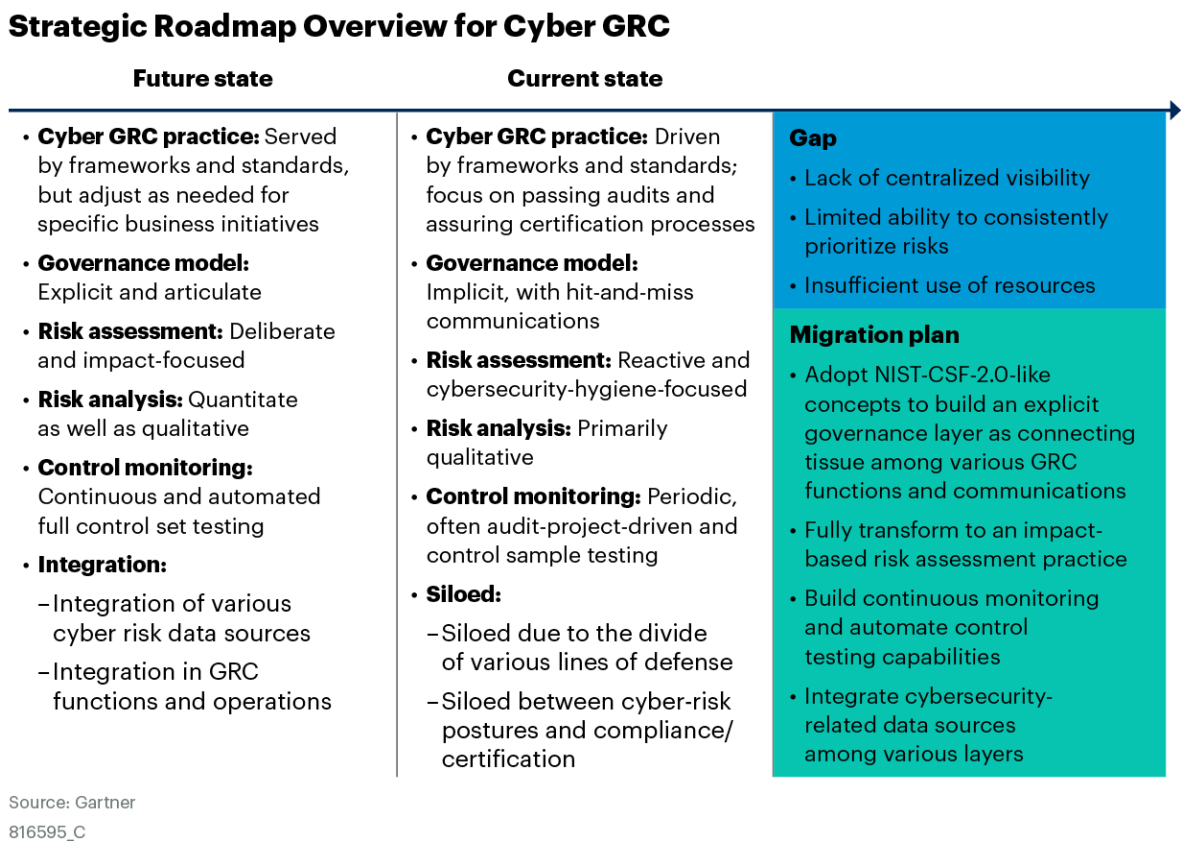
Table 1: Input and Outcome of Impact-Based Cyber GRC

Input	Outcome
■ Clear business direction on cyber-risk appetite ■ Enhanced understanding of cyber impact on business goals and contexts ■ Prioritized protection of key business elements ■ Alignment with industry standards and practices ■ Effective securing of critical assets ■ Adaptability to evolving risk landscape	■ Clear strategic direction for cyber-GRC-Informed decision making based on potential impact ■ Optimized resource allocation for cybersecurity efforts ■ Agile cybersecurity strategy responsive to business and risk changes

Source: Gartner (October 2024)

This research offers guidance on the key areas of focus for SRM leaders to evolve their cyber GRC practice. Figure 2 offers an overview of this strategic roadmap. The guidance offers a comparison between a future state and the current state, identifying opportunities to evaluate organizational and technology changes and bridge the growing gaps that SRM leaders are facing in cyber GRC. The migration plan recommends, in order of priority, the actions that SRM leaders should take to achieve a modern approach to dealing with cyber risks, compliance obligations and governance structure. Please note: Each organization should pick and choose what makes the most sense in focused areas, as well as for their priorities.

Figure 2: Strategic Roadmap Overview for Cyber GRC



Source: Gartner
816595_C

Gartner

Future State

As new AI technology, like Microsoft Copilot, Google Gemini, Amazon Q and ChatGPT, begins to be piloted and integrated into the digital environment, and as regulators put more guardrails in place (e.g., SEC disclosure rules, NIS 2 cybersecurity rules, AI regulations), the role of SRM leaders in collaborating with business value chains increasingly becomes a necessity. The overall risk management of an organization demands greater integration from cybersecurity, and a strategically focused cyber GRC effort can facilitate this effectively in the future (i.e., 2025 and beyond; see Table 2).

Table 2: Cyber GRC Future State

(Enlarged table in Appendix)

Characteristics of the function	Explanation
Served by frameworks	While frameworks and standards provide a solid foundation, organizations should view them as tools, not ultimate goals. Organizations should go beyond the baseline capabilities outlined in the frameworks and standards and consider additional measures to enhance their cyber GRC practices. This may include combining data sources from assessments and audits, metrics, and indicators from monitoring and measuring, and incorporating lessons learned from incidents and breaches.
Explicit governance model	In an explicit governance model, clear policies, procedures and reporting lines are established within an organization's context to ensure accountability and consistency in cybersecurity practices. This includes defining the roles, responsibilities and decision rights of risk owners; identifying key stakeholders; establishing decision-making processes; and implementing mechanisms for ongoing monitoring and reporting. By transitioning to an explicit governance model, organizations can improve the effectiveness of their cyber GRC efforts. This provides clarity, accountability and consistency in cybersecurity practices, ensuring that cyber risks are properly managed and aligned with business objectives.
Deliberate and collaborative risk assessment	To enhance the effectiveness of risk assessments, it is important to adopt a more proactive and strategic approach. This involves considering a wider range of cyber risks, including emerging threats and vulnerabilities, and assessing their potential impact on the organization's critical assets and strategic objectives. A comprehensive risk assessment should also consider the broader business context, including regulatory requirements, industry standards and customer expectations. It should align with the organization's risk appetite and take into account the evolving cyber-risk landscape. Furthermore, integrating cyber-risk assessments into the overall risk management framework and governance structure of the organization is crucial. This ensures that cyber-risk assessments are conducted regularly, results are explicitly communicated to and accepted by risk owners and relevant stakeholders, and appropriate risk mitigation measures are implemented.
Qualitative and quantitative combined risk analysis	By combining qualitative and quantitative risk analysis methods, organizations can optimize their investments in assessments by triaging the risk exposure, and gain a more contextualized and comprehensive understanding of cyber risks and make more-informed decisions. Qualitative analysis provides insights into the nature and context of risks, while defensible quantitative analysis adds a more objective and measurable dimension to risk assessment.
Continuous and near-real-time monitoring	Continuous control monitoring involves the real-time or near-real-time monitoring of controls to detect and address any deviations or anomalies as they occur. It uses automated tools and technologies to continuously monitor and assess the effectiveness of controls, providing immediate feedback on control performance. In practice, it reduces the time and effort required for manual assessments.
Data integration	Data integration correlates and analyzes data from different cybersecurity and IT systems and sources, such as vulnerability scanners, threat intelligence feeds, security incident logs and compliance reports. This is done to gain a comprehensive view of the cyber-risk landscape and make informed decisions based on accurate and up-to-date information. Integration also means the incorporation of cyber GRC within the organization's overall GRC program architecture, such as embedding it into the organization's overall ERM framework. This integration allows for coordination and collaboration between the different functions and departments involved in managing cyber risks. It also enables the program to leverage existing processes and structures, ensuring a more efficient and effective approach to cyber GRC.

Source: Gartner (October 2024)

Current State

Organizations often adopt a mix of frameworks and standards for cyber GRC, leading to process inconsistencies and unconnected risk registers across different domains. SRM leaders engage with other risk domains and key leaders on an ad hoc basis, while believing they are accountable for the cyber risk facing the organization. Cyber GRC practices are driven by external compliance mandates and IT asset-focused risk evaluations, with limited guidance linking them to broader business objectives. Various tools, often including Excel spreadsheets, are used, lacking a standardized and integrated toolset for managing and tracking cyber risks (see Table 3).

Table 3: Cyber GRC Current State

(Enlarged table in Appendix)

Characteristics of the function	Explanation
Driven by frameworks	Frameworks and standards play a crucial role in cyber GRC. They provide a structured approach and guidelines for organizations to establish effective cybersecurity practices. However, when an organization is driven by frameworks and standards, they dictate the organization's approach to cybersecurity. The organization's cybersecurity practices and processes are primarily shaped and influenced by the requirements and recommendations outlined in the frameworks and standards to which they adhere. The organization may prioritize compliance with these frameworks and standards as the main objective of their cybersecurity efforts. This approach may result in less focus on risk or inconsistent risk management methods.
Implicit governance model	Governance practices and decision-making processes, when implicit, are often ad hoc, misplaced or based on informal arrangements. The responsibility for cybersecurity governance is typically distributed among various individuals or departments without clear accountability or oversight. This could lead to inconsistencies, gaps and inefficiencies in cybersecurity practices. An implicit governance model can pose challenges in effectively managing cyber risks and aligning cybersecurity efforts with business objectives. Without a clear governance structure, it can be difficult to establish accountability, ensure consistent practices, and effectively communicate and coordinate cybersecurity initiatives.
Reactive and cybersecurity hygiene-focused risk assessment	This method of assessing cyber risks is primarily focused on identifying and addressing immediate vulnerabilities and weaknesses in an organization's cybersecurity practices. This approach typically involves conducting periodic assessments or audits to identify gaps in cybersecurity controls and practices, and taking corrective actions to mitigate those risks. While this approach is important for maintaining a baseline level of cybersecurity hygiene and addressing known vulnerabilities, it has limitations. It tends to be passive in nature, meaning that the assessment is generally conducted to address generic risks with standardized critical controls, rather than proactively identifying and mitigating contextualized potential risks. This can leave organizations vulnerable to emerging threats and evolving attack vectors. Additionally, a "hygiene-focused-only" risk assessment approach may not consider the broader business context and strategic objectives of the organization. It may overlook the potential impact of cyber risks on critical business processes, reputation and overall business continuity.
Primarily qualitative risk analysis	The limitation of using only qualitative risk analysis is that it provides subjective and qualitative assessments of risks without quantifying their potential impact. While qualitative analysis can provide valuable insights into the nature of risks and their potential consequences, it lacks the precision and objectivity that quantitative analysis offers. Without quantitative analysis, it becomes challenging to prioritize risks, allocate resources effectively and make informed decisions based on the potential impact and likelihood of risks. It also limits the ability to compare risks across different areas or projects within an organization.
Use of indefensible quantitative risk analysis	The inability to defend the data and information used for risk quantification, including assumptions and calculation, leads to a significant erosion of credibility. This deficiency undermines the integrity, methodological rigor, transparency, expert validation and decision-making quality of the risk analysis, or treatment of priority proposals.
Periodic and sampling method for controls monitoring	Conducting periodic assessments or audits to sample and evaluating the effectiveness of controls involves selecting a subset of controls or processes for review at specific intervals, typically based on risk assessments or compliance requirements. This allows for a systematic and structured approach to control assessment by providing a snapshot of control effectiveness at a specific point in time. Since it relies on manual assessments, it is often time-consuming and resource-intensive. More importantly, it may not capture control failures or deviations that occur between assessment periods. It does not provide real-time visibility into control performance.
Limited integration	This condition is caused primarily by the divide among various lines of defense and the separation between cyber-risk postures and compliance/certification efforts. The lines of defense within an organization, such as IT operations, risk management, compliance and audit, often operate independently, leading to silos in information sharing and collaboration. This can hinder the effectiveness of cyber GRC as each line of defense may have different priorities, objectives and reporting structures. Additionally, the separation between cyber-risk postures and compliance/certification efforts can create silos. Cyber-risk postures focus on identifying and mitigating risks, while compliance and certification efforts primarily aim to meet regulatory requirements. These two areas may not always align, leading to a lack of integration and coordination.

Source: Gartner (October 2024)

Gap Analysis and Interdependencies

Lack of Centralized Visibility

The lack of centralized visibility of cyber risks is a common challenge faced by organizations with an implicit governance model and inconsistent risk and compliance management methodologies. This issue is particularly pronounced in the context of rapidly evolving risks, where SRM leaders and their executive teams struggle to gain a comprehensive understanding of cyber exposure within specific business contexts and projects. This is characterized by:

- Fragmented governance model: When organizations have a fragmented governance model, with cybersecurity responsibilities distributed across different departments or business units, it becomes challenging to have a centralized view of cyber risks. Lack of coordination and communication between these entities can result in siloed risk management practices and limited visibility.
- Inconsistent risk management methodologies: If there is no standardized and consistent approach to risk management across the organization, it becomes difficult to aggregate and compare cyber risks. Inconsistent methodologies for risk assessment, risk measurement and risk reporting can hinder the establishment of a centralized view of cyber risks.
- Rapidly revolving risks: Cyber risks are constantly evolving, with new threats and vulnerabilities emerging regularly. This dynamic nature of cyber risks makes it challenging to maintain centralized visibility. Traditional periodic risk assessments may not capture the real-time changes and emerging risks, leading to gaps in understanding the current risk landscape.
- Limited communication and collaboration: Insufficient communication and collaboration between cybersecurity and IT teams, executive management and business units can contribute to the lack of centralized visibility. If there is a lack of shared understanding and awareness of cyber risks across the organization, it becomes challenging to establish a centralized view.

Limited Ability to Consistently Prioritize Risks

The limited ability to consistently prioritize risks and the low participation in openly discussing and sharing information on perceived cyber risks, threats, or issues can hinder effective cyber GRC practices. This has led to a focus on compliance requirements and policy adherence, rather than actively addressing and approving deviations critical to the achievement of business objectives. This is characterized by:

- Not adopting a risk scoring and prioritization framework: Based on conversations with clients, Gartner has learned that organizations often use ad hoc or siloed methodologies instead of developing a standardized framework for scoring and prioritizing cyber risks based on their potential impact.
- A culture of limited information flow: Within functional areas, information flow may be optimized and transparent. However, across risk domains, that information flow becomes a hit-and-miss situation. There may be multiple risk registers within an organization, without a good design principle to connect them.

- Incomplete risk acceptance process: This refers to the failure to establish a formal process for approving deviations or exceptions from compliance requirements and policy adherence when necessary. When done right, the process should involve relevant stakeholders, such as the risk owner, SRM leader, executive management, and legal or compliance teams, to ensure that exceptions are assessed, justified, and appropriately managed and frequently reviewed.
- Lack of cyber-risk training and awareness: Most publicly traded companies now have mandatory cybersecurity training and awareness programs. Often, however, they are not cyber-risk-focused and do not offer techniques regarding cyber risks, their potential impact and the importance of common risk terms, as well as reporting and addressing them in translated business terms, such as modern security behavior and culture programs (SBCPs).

Ineffective Use of Resources

The ineffective use of resources can result in disjointed, resource-intensive and reactive approaches to cyber-risk management. This prevents organizations from effectively sharing information, maintaining centralized visibility and making informed decisions about their overall risk posture. It is characterized by:

- Fragmented governance: This can lead to the SRM leader trying to manage all the cyber risks, which is unsustainable.
- Limited cyber GRC data integration: Many data sources are valuable to cyber GRC, but may exist in different layers of the organization. In general, these data sources may be connected for specific reporting needs, but the effort could be labor-intensive and the processes of gathering data sources may not be repeatable. Information related to cyber risks and compliance may be trapped in silos, meaning that it is not effectively or not at all shared or communicated across different departments or business units. This lack of information sharing can hinder the organization's ability to gain a holistic view of cyber risks and make informed decisions.
- Lack of automation and tools: Organizations that rely on semimanual processes for risk assessment and reporting may struggle to maintain centralized visibility. Manual processes can be time-consuming, resource-intensive and prone to human error. The absence of automated tools for near-real time risk monitoring and reporting can hinder the ability to gather and analyze risk data in a centralized manner.

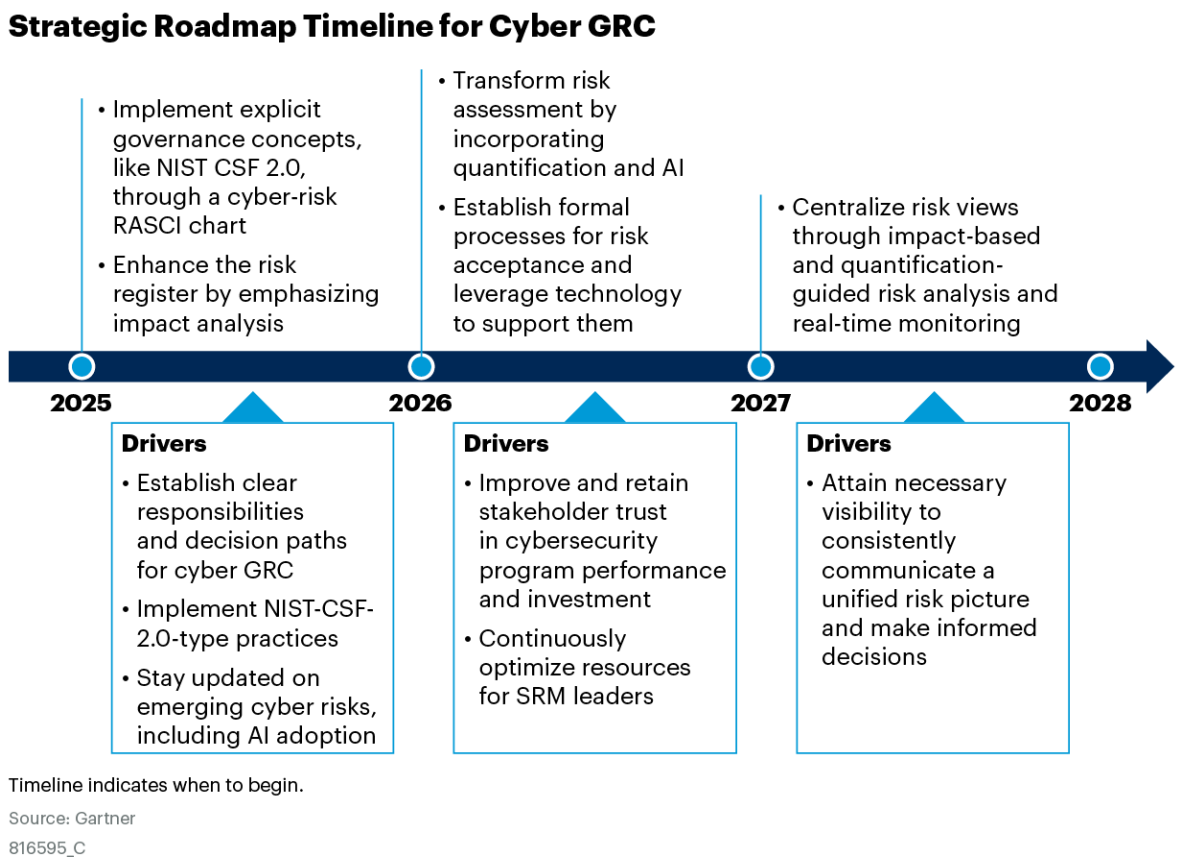
- Audit-driven and certification-focused: This refers to organizations prioritizing compliance with specific regulations or standards in a fragmented manner, without considering the broader context of cyber risks and the organization's overall risk posture. When compliance efforts are approached in isolation, it can result in a disjointed and reactive approach to managing cyber risks. Additionally, it places additional strain on the resources of SRM leaders.

Migration Plan

Based on the gap analysis, Gartner proposes the following roadmap and action items over the next several years to be used as a template for cyber GRC and migration planning suitable for most enterprises. While a different order or parallel approach for providing the end-state success detailed in Figure 3 may be possible, every organization must determine whether a fully integrated cyber GRC approach makes sense for its requirements and, if so, within what time frame.

Organizations cannot expect shortcuts to achieving success in all aspects of their cyber GRC. As such, many larger organizations will explicitly use professional services to assist them in achieving such goals over the next three years. The vast majority of organizations may start from scratch by building a full-time or resource-shared cyber GRC function. This might take a few years, prioritizing areas of greatest opportunity in terms of impact-based risk analysis, a meaningful cyber-risk register and reducing risk through the adoption of a formal risk acceptance process.

Figure 3: Strategic Roadmap Timeline for Cyber GRC



Higher Priority

In the next 18 months, take the following actions.

Transition to Operate With Explicit Governance

The govern function focuses on establishing and maintaining a cybersecurity governance layer and processes. It emphasizes the need for organizations to have a clear understanding of their cybersecurity roles and responsibilities, as well as an alignment of cybersecurity objectives with the overall business goals.

NIST CSF 2.0 added a "govern" layer to enhance oversight, align cybersecurity with business objectives and ensure regulatory compliance, thereby promoting a proactive approach to risk management and resource optimization. This addition builds stakeholder trust and integrates cybersecurity into strategic planning, reinforcing a comprehensive and resilient cybersecurity posture.

The underlying principle of aligning cybersecurity strategy with the organization's goals holds true. It highlights the importance of integrating cybersecurity into the overall governance structure and decision-making processes.

It also emphasizes the need for an approach to cybersecurity that takes into account the organization's unique risk profile, industry regulations, and business objectives. To effectively implement the Govern function, SRM leaders should take these specific steps:

- Formalize the governance committee members and establish a regular cadence for meetings and decision making.
- Emphasize the alignment or even integration of cyber-risk management into ERM. This integration ensures that cyber risks are considered within business context and alongside other business risks, enabling a holistic approach to risk management.
- Create a responsible, accountable, supporting, consulted, informed (RASCI) matrix (see Tool: Cybersecurity Program RASCI Matrix), which explicitly defines the roles and responsibilities of individuals and teams involved in cybersecurity governance. This matrix helps establish clear accountabilities and ensures that everyone understands their role in managing cybersecurity risks.
- Align security initiatives with business priorities and the overall cyber-risk strategy by leveraging Gartner's protection-level agreements (see Use Protection Levels to Create Defensible Risk Appetite Statements).

For further guidance on the importance of governance in cybersecurity, see CISO Effectiveness: Security Operating Models Are Evolving.

Establish Formal Processes for Risk Acceptance and Leverage Technology to Support Them

This action plan is highly dependent on explicit governance as well as an effective cyber-risk assessment practice. A formal process for risk acceptance helps in prioritizing mitigation efforts and allocating resources effectively. SRM leaders should:

- Create a relevant risk appetite statement. Clearly define the criteria for accepting or tolerating risks within the organization. This involves determining acceptable risk thresholds, considering regulatory requirements, and aligning with the organization's risk appetite and business objectives. Using protection-level agreements (PLAs) — measured with outcome-driven metrics — SRM leaders can create new opportunities to redefine risk appetite and govern cybersecurity investments with greater clarity and defensibility (see Use Protection Levels to Create Defensible Risk Appetite Statements).
- Establish risk acceptance processes. Develop formal processes and workflows for evaluating and accepting risks. This leverages the explicit governance structure and brings key stakeholders into the decision-making process. Clearly document the steps involved, roles and responsibilities, and criteria for risk acceptance to retrofit the RASCI matrix.
- Leverage cyber GRC technology solutions. Utilize technology solutions to support and automate risk acceptance processes. This can include risk management software, workflow management tools and integrated GRC platforms. These tools can streamline the risk acceptance workflow, provide visibility into the status of risk acceptance decisions, and facilitate documentation and reporting (see Innovation Insight: Cyber GRC Streamlines Governance).
- Integrate risk acceptance processes with the cyber-risk register. This ensures that accepted risks are properly documented, tracked and monitored over time. It also allows for the identification of any changes in risk acceptance status or the need for reassessment.

Merge Compliance and Risk Management Efforts by Adopting Continuous Control Monitoring

Cybersecurity continuous control monitoring (CCM) is a process that involves the ongoing monitoring and assessment of security controls to ensure their effectiveness and adherence to cybersecurity policies, standards and regulatory requirements. It is a proactive approach that aims to identify and address security vulnerabilities, threats and incidents in real time or near real time.

CCM involves the continuous collection, analysis and reporting of security-related data from various sources, such as security tools, logs and system events. This data is compared against predefined security baselines or benchmarks to detect any deviations or anomalies that may indicate potential security risks or noncompliance with security policies.

CCM integrates compliance and risk management efforts by aligning control monitoring with risk assessments. This ensures that compliance activities are driven by risk priorities and that risk management strategies are informed by compliance requirements. With CCM, organizations will achieve the following capabilities:

- Risk-based approach: CCM allows for a risk-based approach to compliance and risk management. By monitoring controls continuously, organizations can identify potential vulnerabilities and risks promptly, enabling proactive mitigation and reducing the likelihood of security incidents.
- Timely issue detection and remediation: With CCM, organizations can detect control failures or deviations in real time. This allows for immediate remediation actions, minimizing the impact of potential security incidents and reducing the time window for attackers.
- Data-driven decision making: CCM provides SRM leaders with valuable data and insights into control effectiveness, compliance status and potential risks. This data can be utilized to make informed decisions regarding control improvements, resource allocation and risk mitigation strategies.

This approach enables proactive identification and mitigation of risks while maintaining ongoing compliance with regulations and standards. CCM is supported by technology tools; to learn about the details of these tools and use cases, see Innovation Insight: Cybersecurity Continuous Control Monitoring.

Mature Cyber GRC Practice Through Investing Further Automation

Cyber GRC technologies refer to the tools that automate and standardize the implementation of cyber GRC. These tools are designed to automate and streamline various aspects of cyber GRC disciplines, enhancing accuracy, effectiveness and efficiency.

Cyber GRC tools are designed to serve the needs of SRM leaders. These tools generally offer the following differentiated capabilities:

- Continuous, near-real-time data collections
- Management of cybersecurity-specific frameworks and standards
- Framework crosswalk
- Cyber GRC process workflow automation
- Measurement and communication of cyber risks against strategic business goals
- CCM
- Cybersecurity continuous compliance automation (CCCA)
- Cyber-risk quantification (CRQ)
- Linkage to cyber insurance strategy
- Cybersecurity program performance management (CPPM)
- Vulnerability management/threat intelligence (VM/TI)
- Incident response (IR)
- Continuous threat exposure management (CTEM)

SRM leaders should choose a cyber GRC tool that:

- Aligns with organizational needs and integrates with the existing IT and control infrastructure, and evaluates the connectors and low- or no-code integrations. Invest in role-based training to ensure effective use of the cyber GRC tool, focusing not only on tool operation but also on the underlying principles of cyber GRC.

- Involves stakeholders from business, legal compliance and operations in the evaluation process to ensure that the cyber GRC tool aligns with overall organizational objectives and supports broader strategies, not just cybersecurity technical goals.

- Involves enterprise architecture in the early evaluation process for setting up a common data model and reporting configuration.

For specific guidance on cyber GRC tools, see Innovation Insight: Cyber GRC Streamlines Governance.

Medium Priority

In the next 36 months, take the following actions.

Transform Cyber-Risk Assessment by Incorporating Cyber-Risk Quantification and AI-Assisted Risk Analysis

Cyber-risk quantification (CRQ) is a method of expressing risk exposure from an interconnected digital environment to an organization in business-relevant terms (for example, from ordinal scale expressions of probability/impact to advanced statistical modeling of annualized loss expectancy and advanced analytics).

Combining CRQ with more classic qualitative analysis in the digital era for cyber-risk assessment is a necessity. Among Gartner clients, there is plenty of evidence that leading cybersecurity programs have invested in CRQ (see Infographic: Benchmarking Cyber-Risk Quantification — Models, Use Cases and Outcomes).

SRM leaders should consider the following CRQ top practices:

- Increase the benefit of CRQ by focusing on high-value use cases, such as prioritizing significant security investments and cyber insurance.
- When discussing CRQ with business leaders, link risks to business outcomes and highlight the potential impact.
- Triage for an appropriate risk analysis methodology based on the complexity and precision required. For example, if a Monte Carlo model isn't necessary, choose a less complex analysis option.
- Initiate CRQ by analyzing business assets using objective data from existing business impact analysis and monitoring capabilities, instead of subjective probability estimates based on historical incidents or rare events.
- Collaborate with other risk domains to provide a more integrated perspective on risk mitigation options.
- Invest in proofs of concept to validate whether CRQ will gain sufficient buy-in. Consider vendors' AI-based suggestions for best practices to improve your approach, and verify these capabilities before making an investment.

In addition to CRQ, AI in cyber-risk management can optimize assessment and monitoring processes and improve real-time communication. The capabilities include:

- Enhancement of controls implementation
- Identification of deficiencies and triggering adjustment
- Risk monitoring by continuously checking for compliance, spotting potential issues and suggesting actions
- Cybersecurity framework mapping
- Risk reporting by collecting and analyzing cyber-risk data for informed decision making and effective oversight

To leverage these emerging and fast-evolving AI-related capabilities, SRM leaders should consider:

- Developing a comprehensive data strategy that addresses data quality, accessibility, security and privacy considerations. Start by clearly articulating the desired outcome and identify specific use cases where AI can add value in cyber-risk management.

- Assessing data quality and availability, technical infrastructure, organizational culture, and expertise in AI technologies.
- Checking in with your existing cyber GRC vendors and evaluating what types of AI-driven capabilities they already have. Request customer adoption stories and their AI-driven product roadmaps.
- Starting with small-scale proofs of concept to demonstrate the feasibility and value of AI in cyber-risk management. Gradually scale up as confidence in AI technologies grows and organizational capabilities improve.
- Improving existing metrics, such as cost savings and compliance levels for continuous assessment and monitoring, to measure the outcomes of AI-driven cyber-risk management solutions.
- Navigating the hype around AI by focusing on what is already being adopted by real customers versus what's just on the roadmap.

Improve the Cyber-Risk Register by Including the Right Elements

A cyber-risk register is a centralized repository that captures and tracks cyber risks across the organization. It systematically documents elements such as risk taxonomy, risk owners, relevance and tolerance, and inherent and residual risk, mitigating controls and their effectiveness and open issues.

A cyber-risk register should effectively capture and prioritize risks informed by a business impact analysis (BIA; see Figure 4 for a checklist to reference).

Figure 4: A Checklist for What Good Looks Like in a Cyber-Risk Register

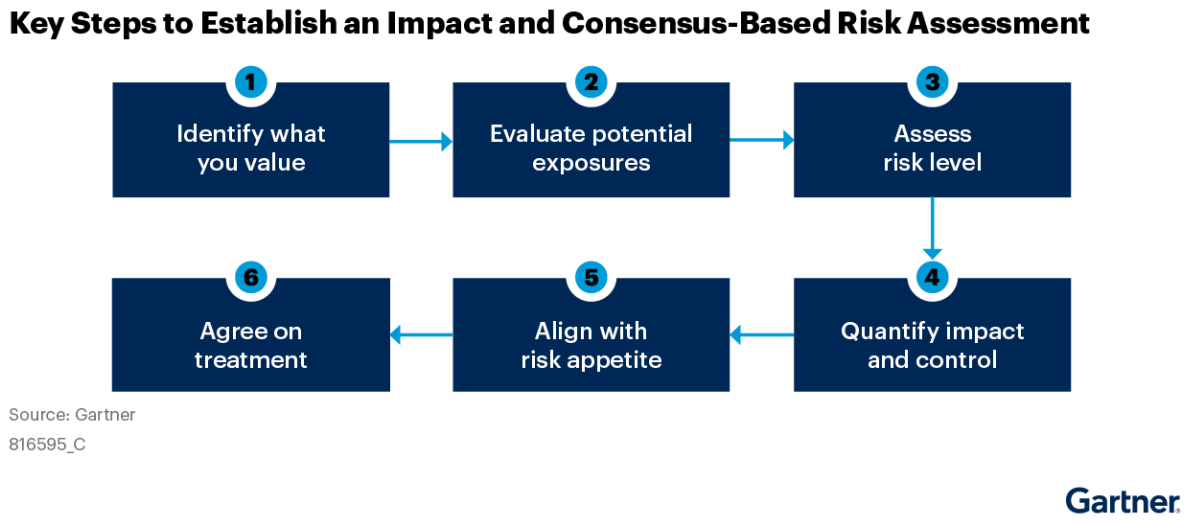
Regularly reviewing, updating and presenting the cyber-risk register to stakeholders and committees, based on changes in the threat landscape, emerging technologies and regulatory requirements, is essential to maintaining its accuracy and relevance. This helps organizations stay resilient and better prepared to mitigate potential threats.

Establish an Impact-Based Risk Analysis

This action involves further integrating cybersecurity into the organization's governance framework and decision-making processes. Cybersecurity efforts must always be in line with the organization's strategic objectives and risk appetite. This enables the identification of critical assets and systems that require heightened protection, allowing for the allocation of resources accordingly. It is important to continuously monitor and update the risk assessments as new data becomes available or the risk landscape changes. This ensures that the assessments remain accurate and up to date.

To achieve this may seem to be daunting. SRM leaders should consider the following key steps for cyber-risk assessment, including identifying what is valued, evaluating potential exposures, assessing risk level, agreeing on treatment, aligning with risk appetite and quantifying impact and control (see Figure 5). These can't be achieved in the short term and require consistent commitments. After all, they represent strategic directions and should not be treated as a project plan.

Figure 5: Key Steps to Establish an Impact and Consensus-Based Risk Assessment



1. **Identify what you value.** Do this to understand the critical assets; data, systems and processes that are essential to the organization's operations and reputation. By identifying, prioritizing and contextualizing these valuable assets, you can focus your risk assessment and mitigation efforts on protecting what matters most. Often, this is achieved with BIA as well as via business risk appetite/acceptance evaluation. Additionally, consider the organization's strategic objectives, industry regulations and compliance requirements.

2. **Evaluate potential exposures.** Do this to identify and assess the specific risks that the organization may face in relation to its critical assets, systems and processes. The evaluation should consider both internal and external factors that could pose a threat to the organization's cybersecurity. Internal factors may include vulnerabilities in systems, inadequate security controls or employee negligence. External factors may include emerging cyberthreats, regulatory changes or supply chain risks. See Gartner's research on CTEM (Implement a Continuous Treat Exposure Management [CTEM] Program and How to Respond to the Threat Landscape in a Volatile, Complex and Ambiguous World) for more details.

3. **Assess the risk level.** Do this to evaluate the identified risks based on their potential impact and likelihood. The risk level can be the basis on which to prioritize efforts and allocate resources accordingly. The assessment should consider factors such as financial impact, reputational damage, operational disruption and regulatory compliance (see Table 4). Assigning a risk level or score to each identified risk helps in determining the severity and urgency of the risk, allowing organizations to focus on addressing the most critical risks first.

4. **Quantify impact and control.** Do this to assign numerical values or scores to the potential impact of a risk event and the effectiveness of existing controls in mitigating that risk. Quantifying the impact helps in understanding the potential financial, operational or reputational consequences of a risk event. Quantifying the control effectiveness provides insights into the level of protection provided by existing controls.

5. **Align with risk appetite.** Once risks have been quantified and their impact and control effectiveness have been assessed, SRM leaders need to compare these results with the organization's predetermined risk appetite. Risk appetite refers to the level of risk that an organization is willing to accept or tolerate. It should mostly come from the business rather than cybersecurity or IT. By aligning the quantified risks with the risk appetite, SRM leaders can determine whether the identified risks fall within acceptable levels or if additional mitigation measures are necessary. This step helps SRM and business leaders make informed decisions about risk acceptance, risk transfer and risk mitigation strategies to ensure that the overall risk exposure remains within acceptable limits.

6. **Agree on treatment.** Do this to consider the various options such as risk avoidance, risk transfer, risk mitigation or risk acceptance. The decision on treatment should align with the organization's risk appetite and overall risk management strategy. It may involve security or IT teams to implement additional controls, enhance existing controls, transfer risk through cyber insurance or third-party agreements, or the business agreeing to accept certain risks based on a cost-benefit analysis. The agreed-on treatment plan should be documented and communicated to relevant stakeholders to ensure a coordinated and consistent approach to managing cyber risks.

Table 4: Sample Risk Impact Categories

(Enlarged table in Appendix)

Risk Impact Category	Impact Details
1. Financial loss	▪ Thefts of funds or assets ▪ Costs of investigating and mitigating the cyber incident ▪ Legal and regulatory fines
2. Operational disruptions	▪ Downtime of critical systems and services ▪ Disruption of business processes ▪ Loss of productivity
3. Reputational damage	▪ Loss of customer trust and confidence ▪ Negative publicity and media coverage ▪ Long-term damage to brand image
4. Data breach consequences	▪ Loss or compromise of sensitive customer information ▪ Violation of data protection regulations ▪ Legal actions and lawsuits
5. Intellectual property theft	▪ Theft or compromise of proprietary information ▪ Loss of competitive advantage ▪ Impact on research and development efforts
6. Loss of trade secrets	▪ Loss of market advantage ▪ Negative impact on innovation and business strategies
7. Supply chain disruption	▪ Disruption to supply chains due to compromised vendors ▪ Delayed deliveries and increased costs
8. Business continuity challenges	▪ Difficulties maintaining operations during and after an attack ▪ Need for investment in a comprehensive resiliency plan
9. Employee productivity	▪ Loss of employee productivity during and after an incident ▪ Increased workload for IT and security teams
10. Increased insurance costs	▪ Rising cost of cybersecurity insurance premiums ▪ Limited coverage due to increased risks
11. Customer relations	▪ Negative impact on customer relationships ▪ Increased demands on customer support
12. Regulatory compliance issues	▪ Failure to comply with industry specific regulations ▪ Increased scrutiny from regulatory bodies
13. Litigation cases	▪ Costs associated with legal actions for affected parties ▪ Cost to hire legal representation for defense
14. Recovery	▪ Costs associated with recovering systems and data ▪ Investment in cybersecurity improvement for future prevention
15. Stock price volatility	▪ Negative impact on stock price due to perceived vulnerabilities ▪ Shareholders' concerns and reactions
16. Cybersecurity investment pressures	▪ Increased pressures on cybersecurity investment ▪ Balancing cybersecurity investments with other business priorities
17. Damage and destruction of physical property and equipment	▪ Disruption of business operations and loss of production ▪ Costly repairs and replacements
18. Health and personal safety	▪ Employees' well-being and productivity ▪ Company reputation, compliance fines and lawsuits

Source: Gartner (October 2024)

Lower Priority

Lower priority strategic considerations can vary depending on the specific needs and circumstances of an organization. Following are some tasks that are often considered lower priority in comparison to the previously outlined areas of focus.

Continuous risk data integration. Beyond CCM and cyber GRC, integrating other relevant data sources for the long term is crucial. Refining data models and leveraging additional data sources continuously require significant investment across functions in the long term. The more data that is integrated overtime, the better context and insight can be derived. However, this may involve costs associated with technology implementation, data integration efforts and personnel training.

Organizations should carefully evaluate the potential benefits and costs of further risk data integration. While it may require a consistent investment, the long-term advantages can outweigh the expenses. These advantages include improved risk visibility, enhanced risk assessment capabilities, better identification of emerging threats and more-effective risk mitigation strategies.

A phased implementation approach is recommended, starting with integrating critical data sources in the short term for CCM, for example, and gradually expanding to include additional sources. Collaboration between functions, such as IT, cybersecurity, risk management and compliance, is essential to ensure alignment and optimize resource allocation.

Administrative process optimization. In this area, policy documentation management may be of lower priority. While it is important for maintaining a structured and organized approach to cyber GRC, it may not directly and strategically impact immediate risk management and compliance efforts. Finding a balance between administrative tasks and core cyber GRC goals is essential to ensure a comprehensive and well-functioning cyber GRC practice.

It is important to note that strategic prioritization within a cyber GRC function should be based on the organization's risk profile, compliance requirements and strategic objectives. Regular review and reassessment of priorities is necessary to ensure that focus and resources are allocated effectively.

Acronym Key and Glossary Terms

BIA	business impact analysis
CCCA	cybersecurity continuous compliance automation
CCM	continuous control monitoring
CPPM	cybersecurity program performance management
CTEM	continuous threat exposure management
CRQ	cyber-risk quantification
GRC	governance, risk and compliance
IR	incident response
KPI	key performance indicator
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
RASCI	responsible, accountable, supporting, consulted, informed
VM/TI	vulnerability management/threat intelligence

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Innovation Insight: Cybersecurity Continuous Control Monitoring

Hype Cycle for Cyber-Risk Management, 2024

Innovation Insight: Cyber GRC Streamlines Governance

Succeed as an SRM Leader by Infusing Resilience Into Your Program

Table 1: Input and Outcome of Impact-Based Cyber GRC

Input	Outcome
■ Clear business direction on cyber-risk appetite ■ Enhanced understanding of cyber impact on business goals and contexts ■ Prioritized protection of key business elements ■ Alignment with industry standards and practices ■ Effective securing of critical assets ■ Adaptability to evolving risk landscape	■ Clear strategic direction for cyber-GRC-Informed decision making based on potential impact ■ Optimized resource allocation for cybersecurity efforts ■ Agile cybersecurity strategy responsive to business and risk changes

Source: Gartner (October 2024)

Table 2: Cyber GRC Future State

Characteristics of the function	Explanation
Served by frameworks	While frameworks and standards provide a solid foundation, organizations should view them as tools, not ultimate goals. Organizations should go beyond the baseline capabilities outlined in the frameworks and standards and consider additional measures to enhance their cyber GRC practices. This may include combining data sources from assessments and audits, metrics, and indicators from monitoring and measuring, and incorporating lessons learned from incidents and breaches.
Explicit governance model	In an explicit governance model, clear policies, procedures and reporting lines are established within an organization's context to ensure accountability and consistency in cybersecurity practices. This includes defining the roles, responsibilities and decision rights of risk owners; identifying key stakeholders; establishing decision-making processes; and implementing mechanisms for ongoing monitoring and reporting. By transitioning to an explicit governance model, organizations can improve the effectiveness of their cyber GRC efforts. This provides clarity, accountability and consistency in cybersecurity practices, ensuring that cyber risks are properly managed and aligned with business objectives.
Deliberate and collaborative risk assessment	To enhance the effectiveness of risk assessments, it is important to adopt a more proactive and strategic approach. This involves considering a wider range of cyber risks, including emerging threats and vulnerabilities, and assessing their potential impact on the organization's critical assets and strategic objectives.

	A comprehensive risk assessment should also consider the broader business context, including regulatory requirements, industry standards and customer expectations. It should align with the organization's risk appetite and take into account the evolving cyber-risk landscape. Furthermore, integrating cyber-risk assessments into the overall risk management framework and governance structure of the organization is crucial. This ensures that cyber-risk assessments are conducted regularly, results are explicitly communicated to and accepted by risk owners and relevant stakeholders, and appropriate risk mitigation measures are implemented.
Qualitative and quantitative combined risk analysis	By combining qualitative and quantitative risk analysis methods, organizations can optimize their investments in assessments by triaging the risk exposure, and gain a more contextualized and comprehensive understanding of cyber risks and make more-informed decisions. Qualitative analysis provides insights into the nature and context of risks, while defensible quantitative analysis adds a more objective and measurable dimension to risk assessment.
Continuous and near-real-time monitoring	Continuous control monitoring involves the real-time or near-real-time monitoring of controls to detect and address any deviations or anomalies as they occur. It uses automated tools and technologies to continuously monitor and assess the effectiveness of controls, providing immediate feedback on control performance. In practice, it reduces the time and effort required for manual assessments.
Data integration	Data integration correlates and analyzes data from different cybersecurity and IT systems and sources, such as vulnerability scanners, threat intelligence feeds, security incident logs and compliance reports. This is done

	to gain a comprehensive view of the cyber-risk landscape and make informed decisions based on accurate and up-to-date information. Integration also means the incorporation of cyber GRC within the organization's overall GRC program architecture, such as embedding it into the organization's overall ERM framework. This integration allows for coordination and collaboration between the different functions and departments involved in managing cyber risks. It also enables the program to leverage existing processes and structures, ensuring a more efficient and effective approach to cyber GRC.

Source: Gartner (October 2024)

Table 3: Cyber GRC Current State

Characteristics of the function	Explanation
Driven by frameworks	Frameworks and standards play a crucial role in cyber GRC. They provide a structured approach and guidelines for organizations to establish effective cybersecurity practices. However, when an organization is driven by frameworks and standards, they dictate the organization's approach to cybersecurity. The organization's cybersecurity practices and processes are primarily shaped and influenced by the requirements and recommendations outlined in the frameworks and standards to which they adhere. The organization may prioritize compliance with these frameworks and standards as the main objective of their cybersecurity efforts. This approach may result in less focus on risk or inconsistent risk management methods.
Implicit governance model	Governance practices and decision-making processes, when implicit, are often ad hoc, misplaced or based on informal arrangements. The responsibility for cybersecurity governance is typically distributed among various individuals or departments without clear accountability or oversight. This could lead to inconsistencies, gaps and inefficiencies in cybersecurity practices. An implicit governance model can pose challenges in effectively managing cyber risks and aligning cybersecurity efforts with business objectives. Without a clear governance structure, it can be difficult to establish accountability, ensure consistent practices, and effectively communicate and coordinate cybersecurity initiatives.
Reactive and cybersecurity hygiene-focused risk assessment	This method of assessing cyber risks is primarily focused on identifying and addressing immediate vulnerabilities and weaknesses in an organization's

	cybersecurity practices. This approach typically involves conducting periodic assessments or audits to identify gaps in cybersecurity controls and practices, and taking corrective actions to mitigate those risks. While this approach is important for maintaining a baseline level of cybersecurity hygiene and addressing known vulnerabilities, it has limitations. It tends to be passive in nature, meaning that the assessment is generally conducted to address generic risks with standardized critical controls, rather than proactively identifying and mitigating contextualized potential risks. This can leave organizations vulnerable to emerging threats and evolving attack vectors. Additionally, a “hygiene-focused-only” risk assessment approach may not consider the broader business context and strategic objectives of the organization. It may overlook the potential impact of cyber risks on critical business processes, reputation and overall business continuity.
Primarily qualitative risk analysis	The limitation of using only qualitative risk analysis is that it provides subjective and qualitative assessments of risks without quantifying their potential impact. While qualitative analysis can provide valuable insights into the nature of risks and their potential consequences, it lacks the precision and objectivity that quantitative analysis offers. Without quantitative analysis, it becomes challenging to prioritize risks, allocate resources effectively and make informed decisions based on the potential impact and likelihood of risks. It also limits the ability to compare risks across different areas or projects within an organization.
Use of indefensible quantitative risk analysis	The inability to defend the data and information used for risk quantification, including assumptions and calculation, leads to a significant erosion of credibility. This deficiency undermines the integrity, methodological rigor,

	transparency, expert validation and decision-making quality of the risk analysis, or treatment of priority proposals.
Periodic and sampling method for controls monitoring	Conducting periodic assessments or audits to sample and evaluating the effectiveness of controls involves selecting a subset of controls or processes for review at specific intervals, typically based on risk assessments or compliance requirements. This allows for a systematic and structured approach to control assessment by providing a snapshot of control effectiveness at a specific point in time. Since it relies on manual assessments, it is often time-consuming and resource-intensive. More importantly, it may not capture control failures or deviations that occur between assessment periods. It does not provide real-time visibility into control performance.
Limited integration	This condition is caused primarily by the divide among various lines of defense and the separation between cyber-risk postures and compliance/certification efforts. The lines of defense within an organization, such as IT operations, risk management, compliance and audit, often operate independently, leading to silos in information sharing and collaboration. This can hinder the effectiveness of cyber GRC as each line of defense may have different priorities, objectives and reporting structures. Additionally, the separation between cyber-risk postures and compliance/certification efforts can create silos. Cyber-risk postures focus on identifying and mitigating risks, while compliance and certification efforts primarily aim to meet regulatory requirements. These two areas may not always align, leading to a lack of integration and coordination.

Source: Gartner (October 2024)

Table 4: Sample Risk Impact Categories

Risk Impact Category	Impact Details
1. Financial loss	■ Thefts of funds or assets ■ Costs of investigating and mitigating the cyber incident ■ Legal and regulatory fines
2. Operational disruptions	■ Downtime of critical systems and services ■ Disruption of business processes ■ Loss of productivity
3. Reputational damage	■ Loss of customer trust and confidence ■ Negative publicity and media coverage ■ Long-term damage to brand image
4. Data breach consequences	■ Loss or compromise of sensitive customer information ■ Violation of data protection regulations ■ Legal actions and lawsuits

5. Intellectual property theft	■ Theft or compromise of proprietary information ■ Loss of competitive advantage ■ Impact on research and development efforts
6. Loss of trade secrets	■ Loss of market advantage ■ Negative impact on innovation and business strategies
7. Supply chain disruption	■ Disruption to supply chains due to compromised vendors ■ Delayed deliveries and increased costs
8. Business continuity challenges	■ Difficulties maintaining operations during and after an attack ■ Need for investment in a comprehensive resiliency plan
9. Employee productivity	■ Loss of employee productivity during and after an incident ■ Increased workload for IT and security teams
10. Increased insurance costs	■ Rising cost of cybersecurity insurance premiums ■ Limited coverage due to increased risks

11. Customer relations	■ Negative impact on customer relationships ■ Increased demands on customer support
12. Regulatory compliance issues	■ Failure to comply with industry specific regulations ■ Increased scrutiny from regulatory bodies
13. Litigation cases	■ Costs associated with legal actions for affected parties ■ Cost to hire legal representation for defense
14. Recovery	■ Costs associated with recovering systems and data ■ Investment in cybersecurity improvement for future prevention
15. Stock price volatility	■ Negative impact on stock price due to perceived vulnerabilities ■ Shareholders' concerns and reactions
16. Cybersecurity investment pressures	■ Increased pressures on cybersecurity investment ■ Balancing cybersecurity investments with other business priorities

17. Damage and destruction of physical property and equipment	■ Disruption of business operations and loss of production ■ Costly repairs and replacements
18. Health and personal safety	■ Employees' well-being and productivity ■ Company reputation, compliance fines and lawsuits

Source: Gartner (October 2024)