Innovation Insight: Cyber GRC Streamlines Governance

13 August 2024 - ID G00815931 - 24 min read

By Analyst(s): Jie Zhang, Michael Kranawetter

Initiatives:Cyber Risk; Build and Optimize Cybersecurity Programs

The lack of clear business leader expectations on cyber GRC leads to fragmented approaches and scant investment. This research helps security leaders use cyber GRC tools to streamline governance, risk and compliance processes through rapid data collection, integration, monitoring and reporting.

Overview

Key Findings

- Security and risk management (SRM) leaders lack a clear understanding of business leaders' expectations on cyber governance, risk and compliance (GRC) results in piecemeal approaches and inadequate investment in cyber-risk management.
- Eighty-five percent of Gartner clients who use GRC technology have multiple tools in place. When organizations use multiple tools focused on different risk domains, not specifically designed for cyber GRC, data is fragmented, and it is difficult to understand the impact of cyber risks.
- Risk management and decision-making processes are hindered when multiple tools are used.

Recommendations

- Develop a clear picture of your organization's demands (or absence of such demands) in terms of cyber-risk and compliance requirements by engaging with key stakeholders — including IT, legal, compliance and operations — to gather their input and insights.
- Determine the most suitable cyber GRC tools for your organization by engaging with key stakeholders, including IT, legal, compliance and operations, to assess their cyber-risk and compliance needs.
- Evaluate the connectors and low-/no-code integrations of cyber GRC tools to align them to organizational needs and integrate them with existing infrastructure.

Strategic Planning Assumption

By 2027, 75% of cyber GRC tool evaluations will include use cases for continuous control monitoring (CCM), cybersecurity continuous compliance automation (CCCA) and cyber-risk quantification (CRQ).

Introduction

Operating a cyber GRC function is a relatively new and evolving area of responsibility for security and risk management (SRM) leaders. Deciding whether to have a separate cyber GRC apparatus or be absorbed by existing enterprise GRC functions depends primarily on factors such as the industry sector, operating model and the level of dependency on digital technologies. If the cyber GRC function is part of the SRM's function, it should be connected and operated as an integral part of the organization's overall GRC.

However, due to the rapid digitization and the expanding scope of cybersecurity, cyber GRC may emerge within the cybersecurity arena and continue to evolve organically within that context. In such cases, business leaders may be missing a critical linkage. This lack of clear connection can result in an inaccurate scope for the cyber GRC function and missed opportunities for SRM leaders.

Cyber GRC technology refers to the tools that automate and standardize the implementation of cyber GRC. The capabilities included in cyber GRC tools are specifically designed to automate and streamline various aspects of cyber GRC processes, such as IT-asset-based cyber-risk register, cyber-risk assessment workflows, cybersecurity-related frameworks and standards management, cyber incidents response, continuous controls monitoring, and cyber-risk prioritization through quantification. These capabilities can be part of a broader GRC platform or a stand-alone tool.

Our primary focus of this research is on the technology capabilities designed to support a chief information security officer's (CISO's) function and manage cyber risks and cybersecurity compliance requirements, rather than for a broader enterprise GRC.

> **"We have 15 plus different security and risk management tools, and they all work in some shape or form of silos. We don't have a complete cybersecurity program overview of our organization. When mergers and acquisitions (M&A) happen or a new business initiative is in the fast track pipeline, it is very challenging for my team to evaluate the cyber risks involved. Today, managing a cyber GRC function is no longer just about documentation and point-in-time assessments; it requires continuous monitoring and proactive actions. Therefore, real-time and connected data are critically important."**
>
> — *Security and risk leader working in a global retail company*

Organizations often rely on disparate tools not specifically designed for cyber GRC, which can create challenges in achieving a comprehensive view of cyber risks and their impact on the organization. These tools could be point solutions for specific workflow automations such as vendor risk management, IT project risks, security incident management and vulnerability management. This fragmented approach to tooling can result in disconnected data, making it difficult to effectively manage and mitigate cyber risks.

Furthermore, the investment in GRC in general can be fragmented within an organization. Different risk domains and departments may have their own budgets and priorities, leading to a piecemeal approach to GRC where individual projects are focused on specific regulations or compliance requirements. As a result, organizations may implement siloed and overlapping tools, which can further complicate the GRC landscape. Ultimately, whether assembling a set of best-in-class tools or selecting a single, broader GRC platform, there is no right or wrong answer in terms of tool investment to address all GRC requirements throughout an enterprise.

Adopting a unified approach to GRC tooling and investment can have several positive outcomes:

- **Enhanced efficiency and elimination of duplicated efforts —** By using integrated tools to address similar GRC needs across different risk domains, organizations can optimize resources and reduce complexity.
- **Improved integration and coordination —** A unified approach to GRC tooling can establish a comprehensive view of risks and compliance throughout the organization, promoting better understanding and management of these aspects.
- **Effective communication and reporting —** A consolidated approach to GRC tooling can enhance the organization's ability to effectively communicate and report on GRC activities, thereby promoting transparency and accountability.

Common Cyber GRC Tool Evaluation Criteria

When evaluating cyber GRC tools, organizations typically consider several key criteria to ensure they meet their specific needs and requirements. See Table 1 for the common evaluation criteria for cyber GRC tools.

Table 1: Cyber GRC Tool Evaluation Criteria

(Enlarged table in Appendix)

Category	Description
Integration capabilities	Ability to integrate with other cybersecurity and IT systems (e.g., SIEM, IAM, VM)
Real-time monitoring	Capability for continuous, near-real-time data collection and monitoring
Compliance automation	Features for automating compliance processes
Risk assessment and management	Capabilities for identifying, assessing and managing cyber risks
Incident response	Capabilities for managing and responding to cybersecurity incidents
User interface and usability	Ease of use, user interface design and user experience
Reporting and analytics	Advanced data analytics and reporting capabilities
Scalability	Ability to scale with the organization's growth and increasing complexity
Customer support and training	Quality of customer support and availability of training resources
Cost-effectiveness	Overall value for money considering features and pricing
IAM = identity and access management; SIEM = security information and event management; VM = vulnerability management	

Source: Gartner

Description

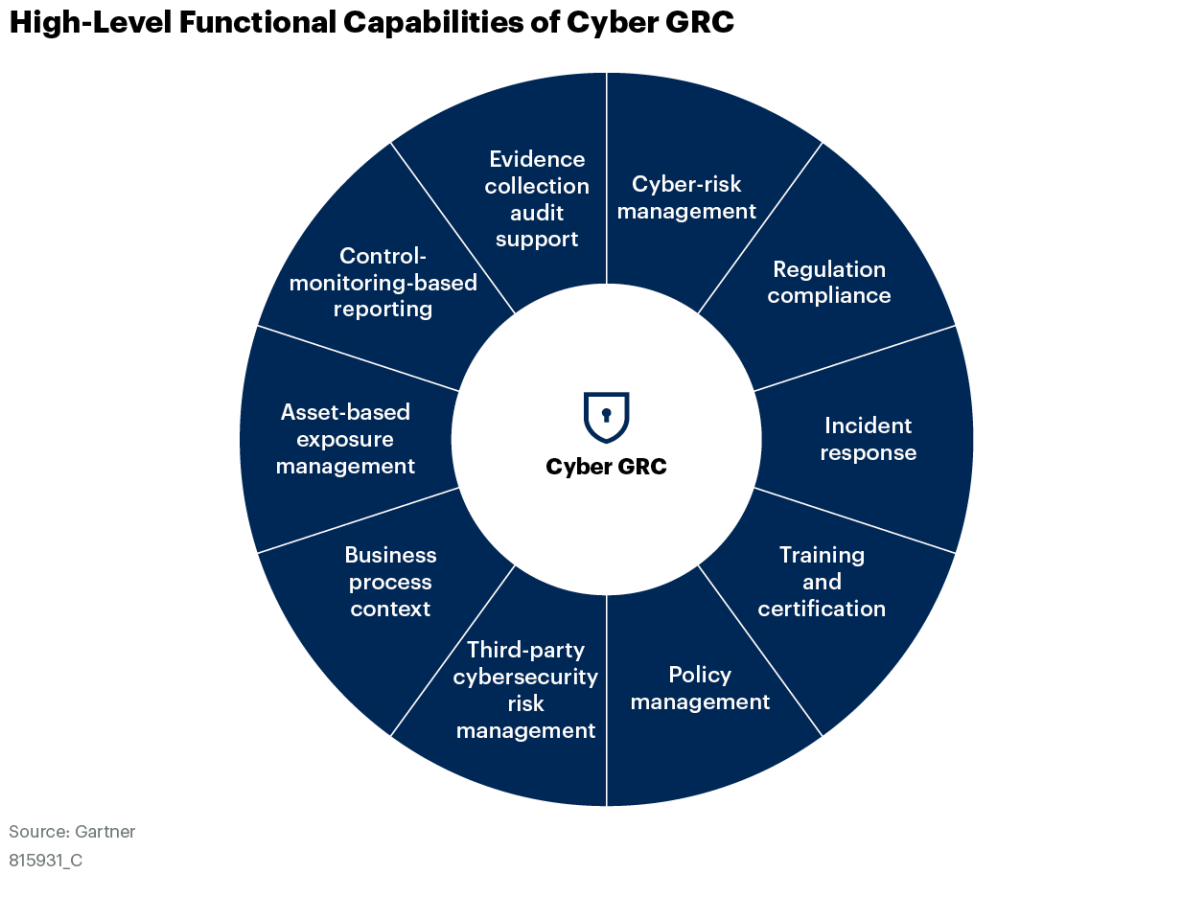
Cyber GRC

Cyber GRC is a strategic framework managed by tools to align business with relevant security regulations, frameworks and standards, while managing risks and regulatory compliance. Governance involves defining leadership, organizational structures and processes that ensure cybersecurity controls are effectively implemented and maintained. Risk management identifies, assesses, mitigates and reports risks, while compliance ensures that the organization meets all legal and policy requirements.

High-Level Capabilities for Cyber GRC

While the specific capabilities of a cyber GRC function may vary depending on the organization's sector, size, operational model, dependency on digital technology, reporting structure and overall maturity, some high-level capabilities are generally important to consider (see Figure 1). These capabilities help organizations manage cyber GRC and address cyber risks while operating within the market-required guardrails.

Figure 1: High-Level Functional Capabilities of Cyber GRC



These capabilities include:

Cyber-Risk Management

Provide a life cycle for assessing the impact of potential risks, justifying its evaluation criteria and implementing appropriate controls. This includes scanning, identifying and prioritizing risks, conducting assessments, and developing mitigation strategies.

Legal and Regulatory Compliance

Help organizations monitor, report and manage cyber compliance requirements. This includes tracking regulatory mandates, implementing and monitoring security controls to ensure adherence to applicable laws, regulations and industry standards.

Incident Response

Support cybersecurity incident response planning and preparedness, including internal and external reporting mechanisms, escalations to crisis management and tabletops and simulations. Use lessons from tabletops, simulations and postincident reports to improve incident response preparedness and cybersecurity measures more broadly. These actions contribute to broader cyber resilience efforts.

Training and Certification

Offer training and secure behavior initiatives to educate employees about cybersecurity risks, policies and best practices and enable cyber judgment. It provides mechanisms for the organization to retain a sufficient level of basic proficiency in independently making cyber-risk decisions and structured pathways for employees to obtain formal certification of their expertise.

Privacy Management

Cooperate with privacy teams to establish controls to comply with privacy regulations, maintain customer trust and mitigate the risk of data breaches involving personal data. This also involves the alignment of processes, policies and practices put in place to ensure the protection and responsible handling of personal data.

Third-Party Cybersecurity Risk Management

Support processes and tools for assessing and managing the cyber risks associated with third parties. This includes conducting due diligence assessments, establishing contractual requirements for cybersecurity controls and monitoring third-party compliance.

Business Process Context

Design an approach that considers the interconnectedness of technology, people and processes within an organization. This involves implementing strategies and controls to identify, assess and mitigate cyber risks and binding compliance requirements that may impact critical business processes and ensure a balanced approach oriented to provide business value.

Asset-Based Exposure Management

Support the identification and assessment of potential risks associated with an organization's assets. This includes tangible assets such as hardware, software and infrastructure, as well as intangible assets like business processes, data, intellectual property and brand reputation. While this research is applicable throughout industries, in physical-assets-heavy sectors, such as transportation and hospitality, it may place a particular emphasis on cyber-physical systems (CPS) and their associated risk management disciplines.

Control-Monitoring-Based Reporting

Ensure a broad scope of controls, including technical and organizational measures and processes, are operating effectively and in line with established policies and procedures and efficiently in terms of securing assets in accordance to their classification. Control-monitoring-based reporting allows organizations to understand and identify any deviations or weaknesses to maintain compliance and mitigate risks.

Evidence Collection Audit Support

Deliver evidence collection and management and facilitate smooth and efficient audits, ensuring that organizations can provide necessary evidence to auditors and regulators. This includes continuous, dynamic and, in the best case, automated collection of documentation, data, indicators and evidence to demonstrate compliance with regulations, standards and internal policies.

From a governance perspective, all data on capabilities is strategically woven into the decision-making mechanisms. This ensures the integration of critical insights into the strategic decisions relevant for the cybersecurity management program.

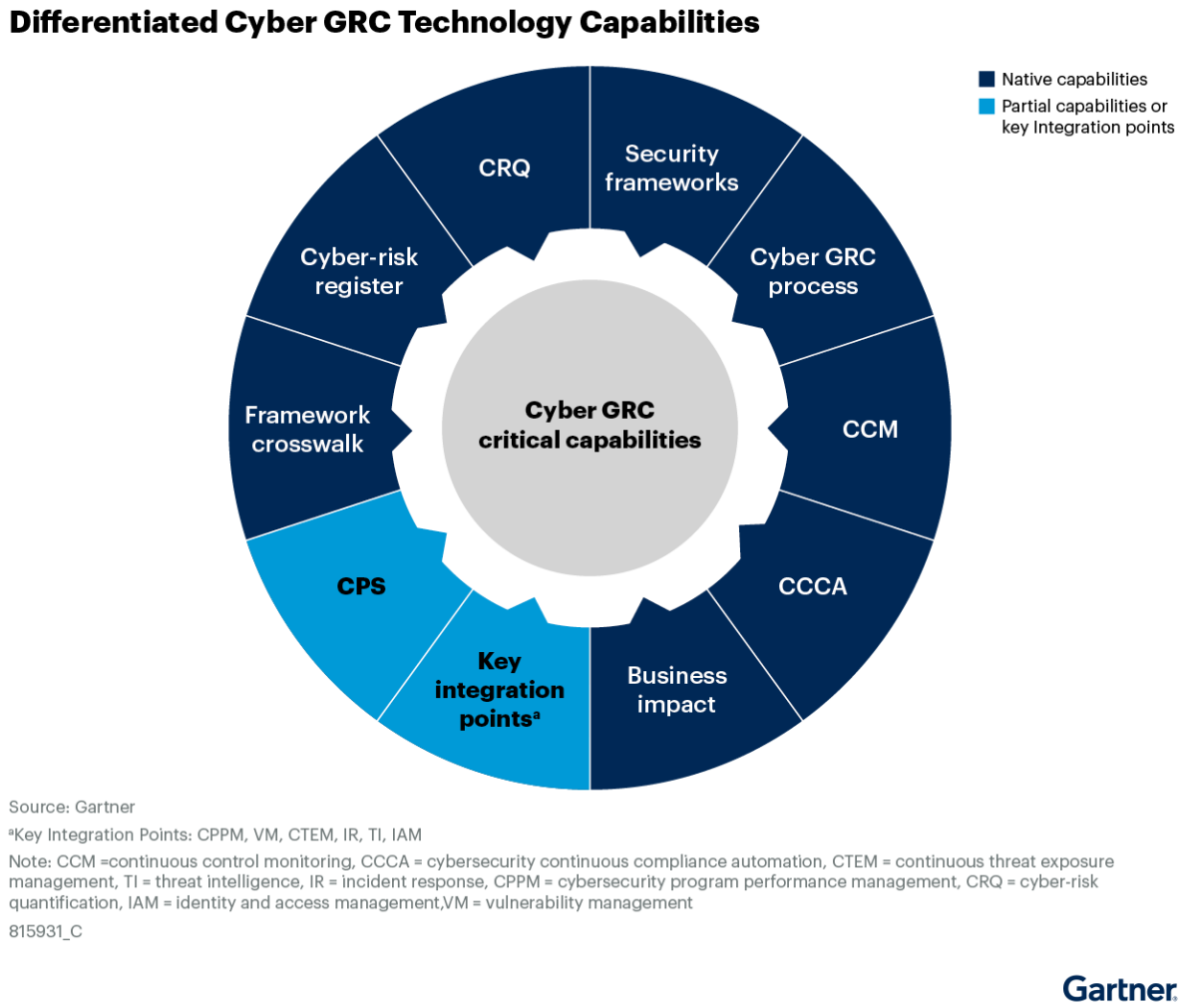
In addition, the cyber GRC capabilities will contribute to tailored reporting offerings. This enables feeding of accurate, relevant and actionable reports into dashboards, each of which is customized to meet the unique needs of different stakeholders.

Benefits and Uses

Cyber GRC Tools Differ From Other GRC tools

Cyber GRC tools offer distinct features and capabilities tailored to the needs of the cybersecurity program and cyber-risk management leaders. They provide centralized management of frameworks and standards, seamless integration with other cybersecurity and IT systems, continuous monitoring, and advanced data analytics and reporting specific to cybersecurity. These features enable organizations to effectively manage cyber risks and ensure compliance in a rapidly evolving threat landscape (see Figure 2).

Figure 2: Differentiated Cyber GRC Technology Capabilities



Differentiated Technology Capabilities

Key Capabilities

- **Continuous, near-real-time data collection** is an essential capability of cyber GRC. It enables organizations to gather and analyze data on cyber risks and compliance in a timely manner, allowing for proactive risk management and decision making.
  - **Continuous control monitoring (CCM)** allows organizations to monitor controls in real time to ensure they are operating effectively. This helps identify and address control failures or weaknesses promptly.
  - **Cybersecurity continuous compliance automation (CCCA)** refers to automating compliance processes to ensure ongoing adherence to regulatory requirements and industry standards. This reduces the burden of manual compliance efforts and helps organizations maintain a continuous state of compliance.

- **Managing cybersecurity-specific frameworks and standards** is another important aspect of cyber GRC. Organizations need to align their cybersecurity practices with industry standards and regulatory requirements. Cyber GRC should provide mechanisms for mapping and implementing these frameworks, ensuring compliance and effective risk management.
    - **Framework crosswalk** refers to the process of mapping different cybersecurity frameworks and standards to identify commonalities and overlaps. This helps organizations streamline their compliance efforts and avoid duplicative work.

- **Cyber GRC process workflow automation** involves automating various aspects of cyber GRC processes, such as risk assessments, compliance monitoring and reporting. Automation improves efficiency, reduces human error and enables organizations to scale their cyber GRC efforts.
- **Cyber-risk register** creates the base for conducting a comprehensive assessment including to identify potential cyber risks that could affect the organization's critical assets, processes and objectives. Entries for cyber risks could include relevances to data breaches, system vulnerabilities, third-party dependencies, regulatory compliance, and more.
- **Measuring and communicating cyber risks against the business's strategic goals** is crucial for business leaders to make informed decisions. Cyber GRC should provide mechanisms for quantifying and communicating cyber risk in a way that aligns with the organization's strategic objectives.
- **Cyber-risk quantification (CRQ)** involves assessing and quantifying cyber risks for alignment to business objectives and regulatory requirements with investments in cyber-risk mitigation. Quantifying cyber risks enables comparison to other business risks and helps decision makers balance risks and opportunities. CRQ supports a cyber-risk management framework by prioritizing risks, facilitating communication to risk owners and executives, and aligning with other risk areas.

Critical Integration Capabilities

- **Cybersecurity program performance management (CPPM)** involves two linked activities in line with business goals: continuous evaluation of cybersecurity functions and strategic planning for improvement. It uses cyber defense planning and optimization (CDPO), automated security control assessment (ASCA) and cybersecurity performance measurement. CPPM helps plan cybersecurity programs and reduces redundancy in controls, processes, operations and mitigation capabilities. It also predicts optimal action and investment in cyber-risk management.

- **The incident response management (IRM)** capability included in a cyber GRC tool is designed to bridge the gap between security operations and the business impact of cyber incidents. This capability involves collecting and analyzing cyber incident data and linking them to the potential business risks they pose. The incident response management capability typically includes features such as incident tracking, workflow management, collaboration tools and reporting functionalities.

- **Threat intelligence (TI)** data provides the necessary context and foundation for identifying and assessing cyber risks, determining the potential impact on the organization and implementing proactive risk mitigation measures. Risk mitigation efforts can be based on the severity of vulnerabilities and the potential impact they pose. TI data helps organizations stay informed about emerging threats and trends.

- The linkage among cyber GRC and **vulnerability management (VM) and continuous threat and exposure management (CTEM)** is essential in creating and validating security operations within the context of the business. It ensures that security efforts are aligned with business objectives, enables proactive risk management and provides assurance of the effectiveness of security measures.

- **Cyber-physical systems (CPS)** present distinct challenges and risks that organizations, particularly those in sectors heavily reliant on physical assets, must address. To effectively manage these risks, cyber GRC tools designed for such organizations should possess integration capabilities. These capabilities enable the correlation of risks that may arise from vulnerabilities and threats impacting the CPS's digital and physical components.

In addition to the above-mentioned technology capabilities, cyber GRC tools are also distinct in the following aspects (see Table 2).

Table 2: Cyber GRC Tools Versus Noncyber GRC Tools

	Cyber GRC	Noncyber GRC
Target role	CISO, other SRM leaders	CRO, CLO, CCO, CFO, Head of ERM
Target risk	Cyber risk	Risks of corporate compliance, finance, market, operations, etc.
Integrated systems	VM, SIEM, TI, IAM, cloud-native security data, task tracking, IT assets, BPM, CPS protection platforms, and audit management	Audit findings, policies, risk assessment, organization structure
Target data	Rapid via streaming data integrations enabling real or near-real-time monitoring	Workflow enabled data collection for mostly quarterly or longer time period

CCO = chief compliance officer; CLO = chief legal officer; CRO = chief risk officer; ERM = enterprise risk management

Source: Gartner

Targeted Buyer and Risk Scope

Cyber GRC tools are specifically and primarily designed for SRM leaders who are responsible for managing cyber risks and ensuring compliance within an organization's cybersecurity arena. The user interface designs, ease-of-use definitions, workflows, data visualization needs, content libraries and more offered by a cyber GRC tool are fundamentally different from a noncyber GRC tool.

Data Source and Integration

Cyber GRC tools often offer substantial API scalability, allowing for seamless integration with cybersecurity and other IT systems. This enables data correlation automation and enhances the overall effectiveness and efficiency of cyber-risk data linkages and risk-sensing time scales.

SRM Leaders Drive Surge in Demand for Cyber GRC Tools Amid Rising Cyber Risks

SRM leaders have not traditionally been the typical buyers of GRC tools. However, with the expansion of digital technologies, evolving cybersecurity threats, increased regulatory and legal mandates, and heightened board oversight, the management of cyber risks has become more complex and resource-intensive. As a result, SRM leaders now play a crucial role in organizations' cyber GRC efforts and are increasingly leading in the selection and implementation of cyber GRC tools.

Every cyber risk should be linked to a business risk in a persistent and meaningful way. Cyber-risk management is now an integral part of modern business management. The growing importance of cybersecurity and cyber-risk management within organizations has also contributed to increased investment and demand for cyber GRC tools. SRM leaders are responsible for overseeing the organization's cybersecurity posture, ensuring compliance with relevant regulations and standards, and reporting to boards and executive teams on the organization's overall secure status. They often rely on cyber GRC tools to streamline and automate processes, assess and manage risks, and demonstrate compliance to stakeholders.

Gartner's experience of receiving numerous inquiries from SRM leaders looking to purchase cyber GRC tools that match their specific needs further supports the growing demand for these tools. As the complexity and importance of managing cyber risks continue to increase, organizations are recognizing the value of investing in specialized cyber GRC tools to effectively address the outlined specifics and their automation requirements.

Key Benefits and Uses

The benefits and uses of cyber GRC tools can greatly enhance an organization's cybersecurity and compliance efforts. Some key benefits and uses include:

- A cyber-risk register serves as a central repository that tracks identified cyber risks and inventories potential threats, vulnerabilities and their associated impacts on the organization's information assets and operations. It typically includes information such as the description of each risk, its likelihood and potential impact, current risk mitigation measures, applied controls and policies, responsible parties, and the status of risk treatment or remediation efforts. It helps organizations gain visibility into the overall risk landscape.

- The automation and streamlining of various cyber-GRC-related processes can reduce manual effort and improve efficiency. This includes tasks such as risk assessments, compliance assessments, policy management, incident response workflows and audit management. For example:
  - CCM helps reduce the manual efforts for security control management, partially relieving staff burden, enabling them to focus on higher-value tasks and reducing costs. CCM provides constant monitoring of security controls, allowing faster detection of potential threats and minimizing breaches and regulatory noncompliance, which prevents significant financial and reputational damage.
  - CCCA offers features and functionalities that streamline and simplify the cybersecurity certification process by not only automating the processes but also linking different entities together and being prevetted by auditors for evidence gathering and reporting, making it more efficient and effective.
- CRQ offers risk assessment by quantifying the potential financial and operational impacts of cyber risks. It helps organizations understand the potential consequences of cyberthreats and make informed decisions regarding risk mitigation strategies and resource allocation.
- Cyber GRC tools are designed to scale with data collection and visualization needs and adapt to evolving cybersecurity threats and compliance requirements. They can accommodate growing data volumes, new regulations and changing business environments.
- Cyber GRC can contribute to cost savings by reducing or eliminating the need for excessive spending on professional services. Traditional approaches to managing cyber risks and compliance often require organizations to engage external consultants or service providers to conduct assessments, audits and other activities. These professional services can be costly and may need to be repeated periodically to ensure ongoing compliance. By implementing a robust cyber GRC function, organizations can internalize many of these activities and reduce their reliance on external professional services.

In addition to the above primary benefits, cyber GRC tools can deliver additional and advanced capabilities:

- Provide capabilities for consistently identifying, assessing and managing cyber risks. More importantly, prioritize risks, track risk mitigation efforts and ensure that appropriate controls are in place to mitigate potential threats.
- By automating relevant processes and providing real-time monitoring and incident response capabilities, cyber GRC tools help organizations strengthen their security posture. They enable proactive identification and response to security incidents, reducing the impact of potential breaches.
- Offer context for reporting and communication via data analytics capabilities, providing organizations with insights into their cybersecurity and compliance performance. They generate comprehensive reports, visualize data and provide metrics to support decision making, demonstrate compliance to stakeholders and identify areas for improvement.
- Many cyber GRC tools include features for assessing and managing the risks associated with third-party vendors and suppliers. They help organizations evaluate vendor security controls, monitor compliance and ensure that vendors meet cybersecurity requirements.
- Cyber GRC tools can provide a structured approach to managing cyber risks and assist in developing a roadmap for improving an organization's cyber-risk management capabilities.

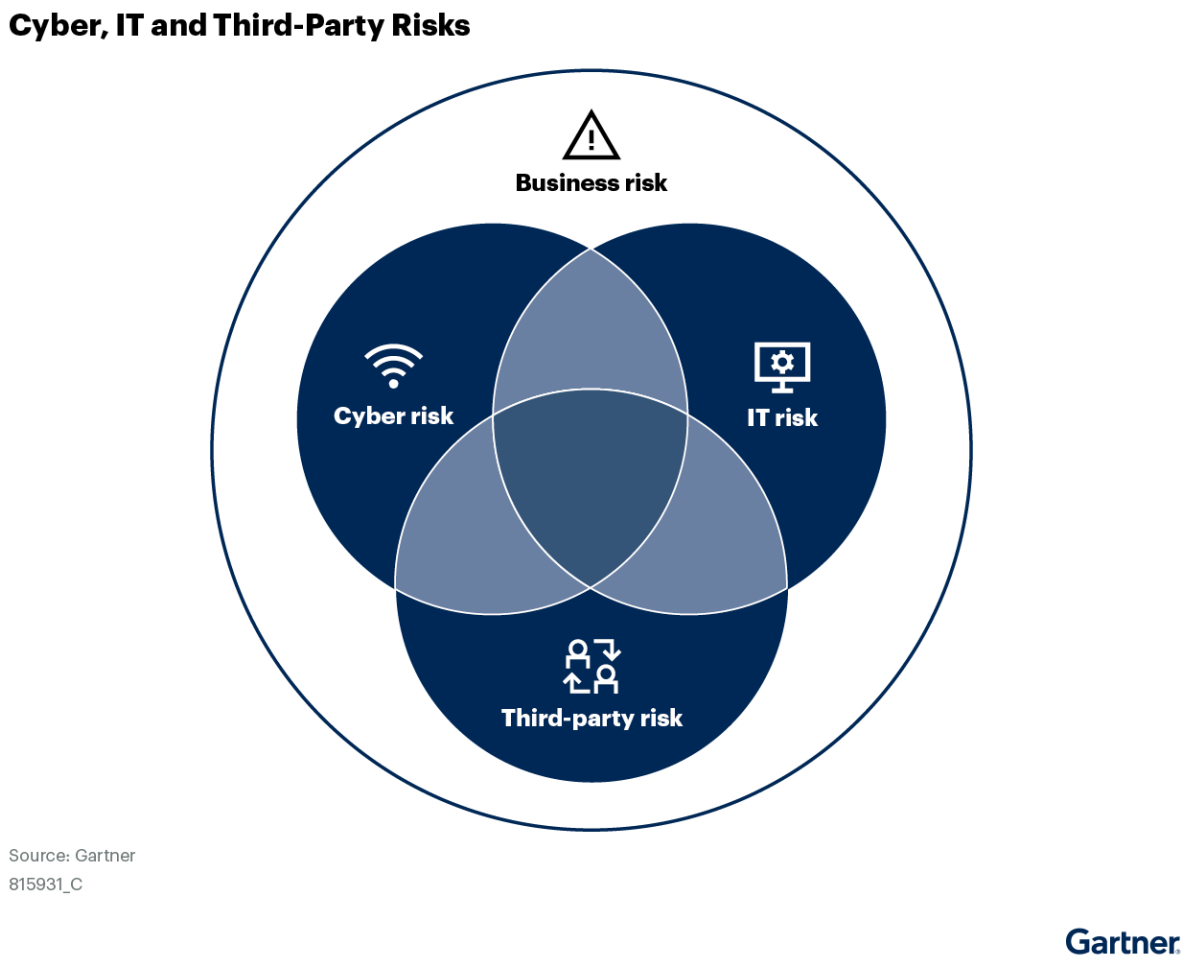
Risks

- Integrating technical and business data sources is a critical capability in cyber GRC, but often it's not thought through or possible in some cases. Without this integration, it is not possible to have a comprehensive view of cyber risks and compliance at the speed at which organizations pursue their digital business goals. Automation within the function relies heavily on the maturity of control and process implementation, as well as the availability of accurate and reliable data.
- Organizations may not consider process changes, role adjustments and training for cyber GRC. To successfully implement cyber GRC, organizations need to invest in all three. These measures equip teams with the necessary skills and knowledge to effectively manage the function. Alternatively, organizations may consider consulting or managed services to augment their capabilities.
- One challenge that organizations may face is the potential overlap in functionality between cyber GRC tools and other GRC or cybersecurity monitoring tools. This can lead to confusion, redundancy and budgetary concerns. Clear communication and coordination between teams involved in procurement and tool selection can help address these issues.
- Aligning IT, security and business objectives can be challenging due to differing priorities and perspectives. It requires effective communication and collaboration between these departments to ensure that cyber GRC aligns with the organization's overall goals.
- Budget constraints and limited financial resources can pose challenges in the implementation and management of cyber GRC tools. The dynamic nature of cyberthreats necessitates continuous updates and upgrades, which can be resource-intensive. Organizations need to carefully allocate their resources to ensure the effective functioning of cyber GRC.
- In hyperscale global organizations, organizations may need to invest in multiple cyber GRC tools to support complex requirements in loosely federated environments. This can add complexity and increase the challenges of managing the function. Organizations should carefully assess their needs and select tools that can effectively address their specific requirements.

Alternatives

There are applicable risk management processes and capabilities that could be adopted by distinctively different risk domains. For example, cyber risk, IT risk and third-party risk could share overlaps in processes and potentially use the same technology platform (see Figures 3 and 4).

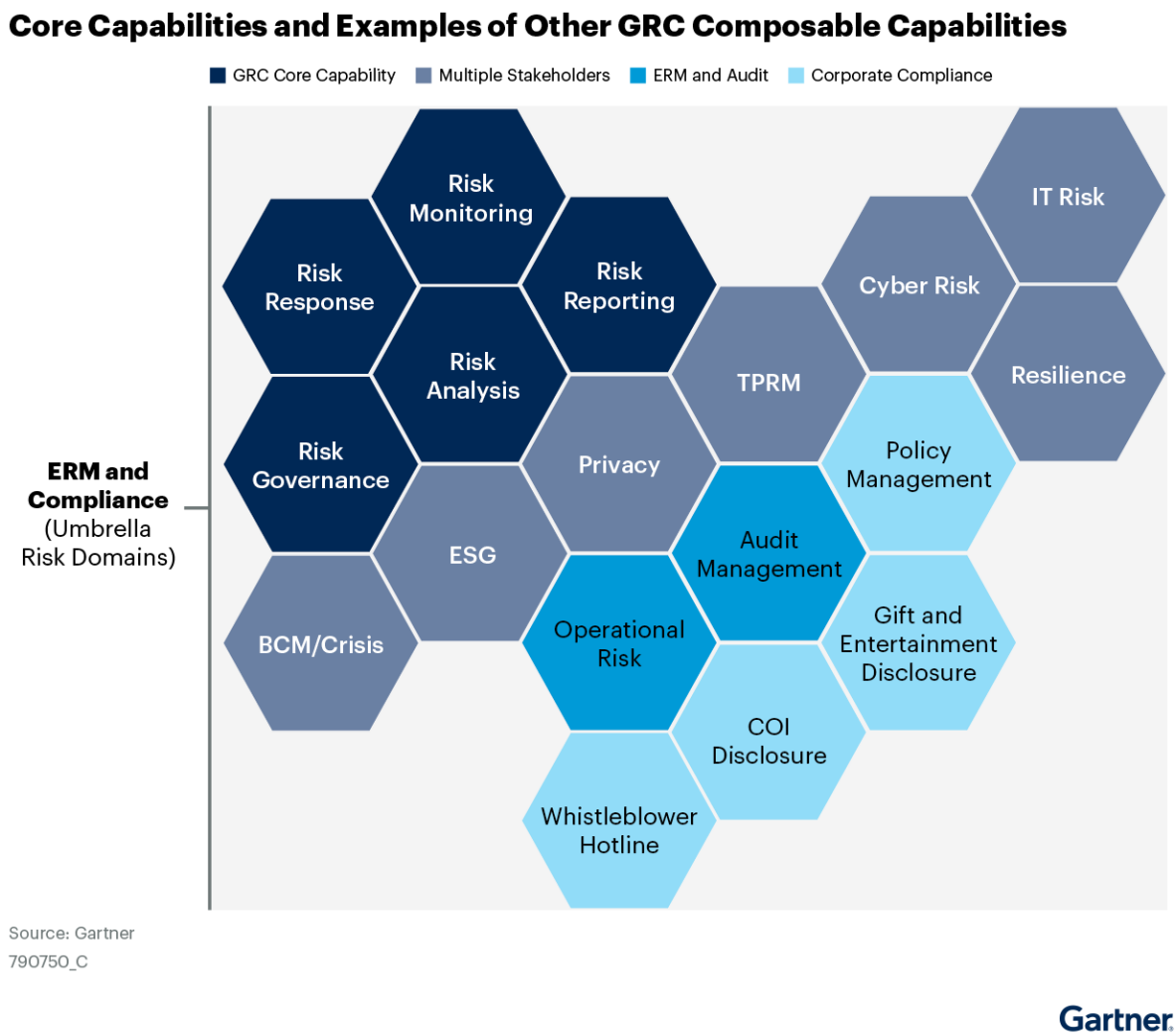
Figure 3: Cyber, IT and Third-Party Risks



Source: Gartner
815931_C

Gartner

Figure 4: Core Capabilities and Examples of Other GRC Composable Capabilities



While alternative tools may offer cyber GRC capabilities or can be extended to automate cyber GRC processes, specialized cyber GRC tools are specifically designed to address the unique challenges and requirements of cybersecurity. However, the following options are viable to some situations (see Table 3).

Table 3: A High-Level Capability Comparison Between Cyber and Noncyber GRC

(Enlarged table in Appendix)

Capabilities	Cyber GRC	Other GRC	Task tools	Excel
Cyber-risk register	5	1	-	-
Cybersecurity-specific frameworks	5	1	1	-
Frameworks crosswalk	4	3	-	-
Cyber GRC workflow automation	5	3	4	1
Business-aligned cyber-risk reporting	5	2	-	-
CCM	5	1	-	-
CCCA	5	2	-	-
CRQ	5	2	-	-
Cyber insurance support	5	-	-	-
CPPM	3	1	-	-
VM/TI	3	-	-	-
IR	4	2	-	-
CTEM	3	2	-	-

This table uses a 0 to 5 scale, where 5 means full support to the capability and 0 means no capability.
Please note: not all the capabilities depicted in the above table are offered by all the relevant cyber GRC tools.

Source: Gartner

Other GRC Tools

When adopting a noncyber GRC tool for managing cyber GRC, consider the following:

- **Adoption already present** — If a generic GRC tool with a dedicated cyber GRC module or capability has already been adopted by other risk functions within the organization (see Market Guide to GRC Tools for Assurance Leaders), leveraging that existing tool can ensure consistency in reporting and streamline overall GRC processes. This can be a viable option if the tool adequately addresses the organization's cyber-risk management needs.
- **Integration capabilities** — If a generic GRC tool has modern application architecture and offers scalability and integration capabilities, it can be considered for managing cyber GRC. If the tool allows for seamless integration of data from security systems and other relevant sources, it can provide a holistic view of cyber risks and enable effective risk management.

- **Organizational mandate —** If your organization has mandated the use of a single GRC platform for reporting purposes and has already invested in a broader GRC platform, extending the usage of the platform may be necessary. However, careful consideration should be given to the upfront investment required for customization or configuration changes, as well as the long-term cost of ownership and support.

Example vendors: Archer, IBM OpenPages, IRM, MetricStream, SAI360, ServiceNow

IT Project Management Tools

When adopting an IT project management tool for cyber GRC, consider the following scenarios:

- **Small shops without a formal CISO function —** In organizations without a dedicated cybersecurity function, the IT department may already have project management tools in place for tracking configuration changes, issues or general task management. In such cases, these existing tools can be utilized to track cyber-GRC-related content and tasks.
- **No budget —** Leveraging an existing project management tool eliminates the need for additional investments in specialized cyber GRC tools. It allows organizations to utilize the capabilities of their existing tool without incurring additional costs.

Example vendors: Jira, ServiceNow

Microsoft Excel Spreadsheets

When to consider the option of doing nothing for the moment and continuing to use Excel spreadsheets?

- **Mostly for nonregulated SMBs —** There is no externally imposed obligation for compliance and no dedicated GRC functions. Cyber GRC is largely about managing a small set of cybersecurity policies, managing issues and tracking incidents.

Recommendations

- Evaluate your cyber-risk and compliance requirements to provide a clear picture of what the organization demands.
- Ensure buy-in from senior stakeholders when choosing a cyber GRC tool, as their support will be crucial for the successful implementation and use of the tool.
    - Choose a tool that aligns with organizational needs and integrates with the existing IT and control infrastructure; evaluate the connectors and low-/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.
- Involve stakeholders from business, legal, compliance and operations in the evaluation process to ensure the cyber GRC tool aligns with overall organizational objectives and supports broader strategies, not just cybersecurity technical goals.
- Involve enterprise architecture in the early evaluation process for setting up a common data model and reporting configuration.

Representative Providers

- Avertro
- Caveonix
- Centraleyes
- CyberArrow
- CyberSaint
- Cyber Sierra
- CyNation
- Cypago
- DigitalXForce
- EGERIRE
- HyperGRC
- LogicGate
- Ostendio
- RiskOptics
- Seconize
- SureCloud
- TrustCloud

Please note: The above list is not exhaustive, and a few of them have extended their technology capabilities outside cyber GRC.

Evidence

The cyber-risk management cohort (four analysts on average) jointly takes over 500 inquiries per year to answer technology “buying” related questions from CISOs or their GRC teams.

Acronym Key and Glossary Terms

API	Application Programming Interface
CCCA	Cybersecurity Continuous Compliance Automation
CCO	Chief Compliance Officer
CCM	Continuous Control Monitoring
CISO	Chief Information Security Officer
CLO	Chief Legal Officer
CPPM	Cybersecurity Program Performance Management
CPS	Cyber-Physical Systems
CRO	Chief Risk Officer
CTEM	Cybersecurity Treat Exposure Management
GRC	Governance, Risk and Compliance
ERM	Enterprise Risk Management
IAM	Identity and Access Management
IR	Incident Response
SIEM	Security Information and Event Management
SRM	Security and Risk Management
TI	Threat Intelligence
VM	Vulnerability Management

Recommended by the Authors

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

Hype Cycle for Cyber-Risk Management, 2024

Best Practices for the Cyber-Risk Management: Plan, Secure and Monitor the Life Cycle

Innovation Insight: Cybersecurity Continuous Control Monitoring

Quick Answer: What CCEOs Should Know About GRC Tools

Table 1: Cyber GRC Tool Evaluation Criteria

Category	Description
Integration capabilities	Ability to integrate with other cybersecurity and IT systems (e.g., SIEM, IAM, VM)
Real-time monitoring	Capability for continuous, near-real-time data collection and monitoring
Compliance automation	Features for automating compliance processes
Risk assessment and management	Capabilities for identifying, assessing and managing cyber risks
Incident response	Capabilities for managing and responding to cybersecurity incidents
User interface and usability	Ease of use, user interface design and user experience
Reporting and analytics	Advanced data analytics and reporting capabilities
Scalability	Ability to scale with the organization's growth and increasing complexity
Customer support and training	Quality of customer support and availability of training resources
Cost-effectiveness	Overall value for money considering features and pricing
IAM = identity and access management; SIEM = security information and event management; VM = vulnerability management	

Source: Gartner

Table 2: Cyber GRC Tools Versus Noncyber GRC Tools

	Cyber GRC	Noncyber GRC
Target role	CISO, other SRM leaders	CRO, CLO, CCO, CFO, Head of ERM
Target risk	Cyber risk	Risks of corporate compliance, finance, market, operations, etc.
Integrated systems	VM, SIEM, TI, IAM, cloud-native security data, task tracking, IT assets, BPM, CPS protection platforms, and audit management	Audit findings, policies, risk assessment, organization structure
Target data	Rapid via streaming data integrations enabling real or near-real-time monitoring	Workflow enabled data collection for mostly quarterly or longer time period

CCO = chief compliance officer; CLO = chief legal officer; CRO = chief risk officer; ERM = enterprise risk management

Source: Gartner

Table 3: A High-Level Capability Comparison Between Cyber and Noncyber GRC

Capabilities	Cyber GRC	Other GRC	Task tools	Excel
Cyber-risk register	5	1	-	-
Cybersecurity-specific frameworks	5	1	1	-
Frameworks crosswalk	4	3	-	-
Cyber GRC workflow automation	5	3	4	1
Business-aligned cyber-risk reporting	5	2	-	-
CCM	5	1	-	-
CCCA	5	2	-	-
CRQ	5	2	-	-
Cyber insurance support	5	-	-	-
CPPM	3	1	-	-
VM/TI	3	-	-	-
IR	4	2	-	-
CTEM	3	2	-	-

This table uses a 0 to 5 scale, where 5 means full support to the capability and 0 means no capability.
Please note: not all the capabilities depicted in the above table are offered by all the relevant cyber GRC tools.

Source: Gartner