Reimagining Cyber Governance, Risk and Compliance (GRC): The Missing Link Between Security and Business Strategy

The better the question. The better the answer.
The better the world works.

Shape the future with confidence

Reimagining Cyber GRC: The Missing Link Between Security and Business Strategy

Cyber Governance, Risk and Compliance (GRC) has often been misunderstood — seen as bureaucratic, reactive and compliance heavy. But when reimagined, it becomes the strategic bridge that unifies cybersecurity, enterprise risk and business growth.

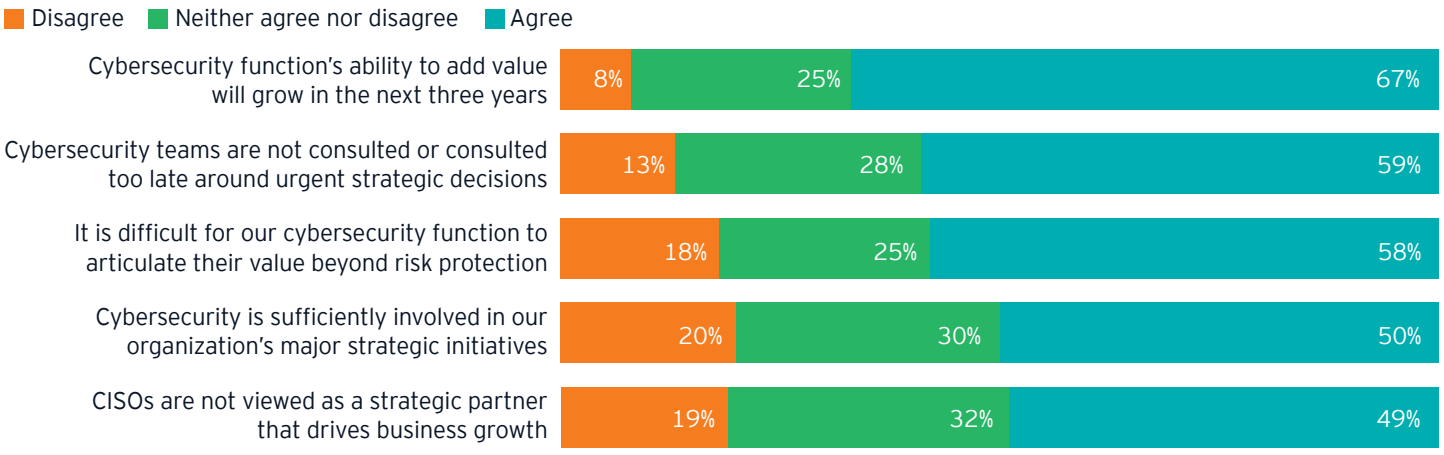
In brief:

- Cyber GRC's legacy perception as a compliance "check-the-box" function keeps it siloed and underleveraged.
- Leading organizations are reframing GRC as the intelligence and orchestration layer for managing cybersecurity in alignment with business objectives.
- Elevated GRC integrates data across cyber domains and translates cyber risk into the language of business strategy.

The Opportunity: GRC as Cyber's Missing Link

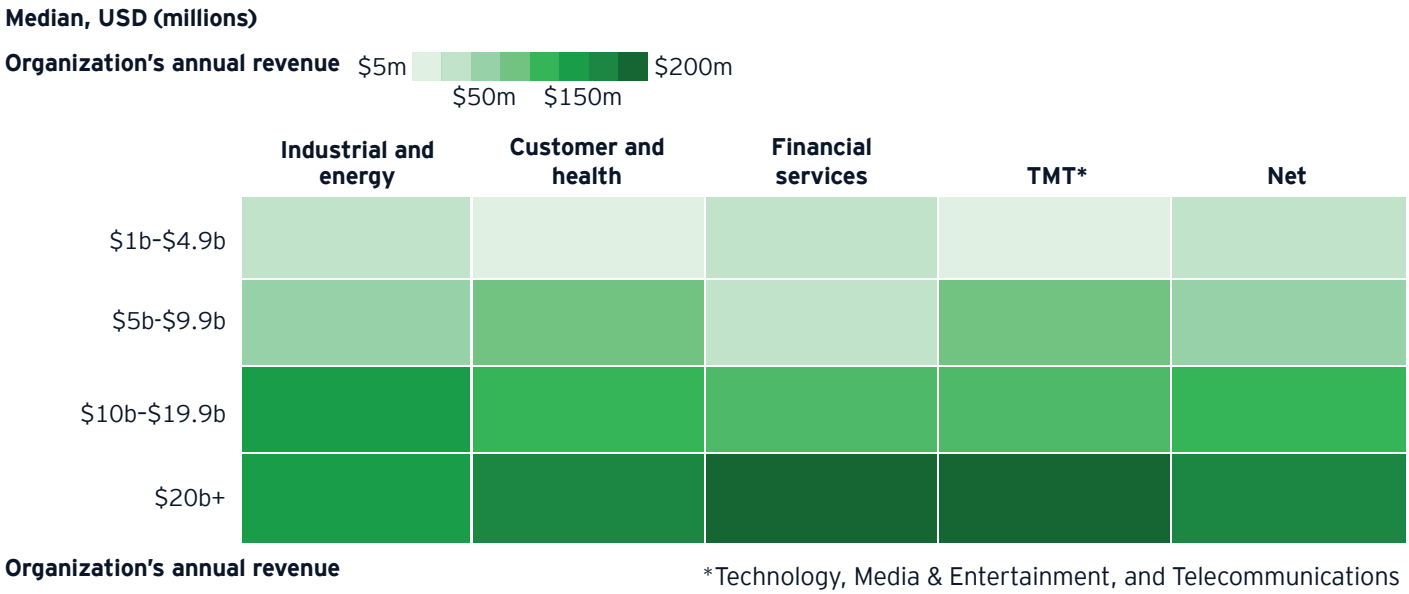
The business value of cybersecurity is clear. When engaged early, chief information security officers (CISOs) deliver 11% to 20% in value to each enterprise-wide strategic area they are involved in (EY 2025). Yet cybersecurity leaders are often invited too late to the table, brought in to "sign off" instead of helping shape business strategy decisions, with just 13% of CISOs consulted at the outset of urgent business decisions (EY 2025). While GRC alone cannot directly reduce risk, it serves as the central engine that orchestrates collaboration across various cyber functions — enabling informed decisions, prioritization and coordinated actions that drive measurable risk reduction.

CISOs find it difficult to articulate their value to the business



[Chart 1: % of CISOs consulted early (13%)] Source: 2025 EY Global Cybersecurity Leadership Insights Study

Cybersecurity functions contribute a median of $36m in enterprise value creation across each business initiative they are significantly involved in



[Chart 2: Value contribution of CISOs per initiative ($36m median)] Source: 2025 EY Global Cybersecurity Leadership Insights Study

This gap is often not about capability but positioning of risk information that can be used to inform and guide business strategy and future financial planning and growth. GRC can change this dynamic. By unifying cybersecurity telemetry data, translating it and mapping it to enterprise priorities, GRC provides the business-ready lens that earns security (and the CISO) a seat in business, strategy-focused conversations. It also enables leading practice risk oversight at the board and executive levels.

The Challenge: Where Cyber GRC Falls Short

Today, GRC's brand problem stems from being seen as slow, compliance heavy and disconnected from business outcomes. This manifests in four ways:

- **Fragmented view of risk**: Cyber teams operate in silos, disconnected from business objectives and outcomes, with no single consolidated view of overall risk posture and exposure.
- **Overemphasis on compliance**: Audit readiness should be viewed with a compliance-focused lens, not as a business risk reduction.
- **Metrics that don't resonate**: Technical jargon dominates, whereas boards need context in terms of financial, operational and reputational impact (EY 2025).
- **Manual and slow**: Static spreadsheets and qualitative ratings lag behind the business and threat landscape in lieu of providing real-time, data-driven, risk-based reporting. The result: Boards and executives see cyber as a cost center. In fact, 58% of CISOs admit they struggle to articulate value beyond risk mitigation (EY 2025).

> "Cyber GRC is no longer just about compliance – it's also about enabling the business to make smarter, faster and more resilient decisions. When risk intelligence is aligned with strategy, security becomes a growth enabler.
>
> – **Saverio Ortizzo**, AVP IT Risk Management and Cybersecurity, Merck

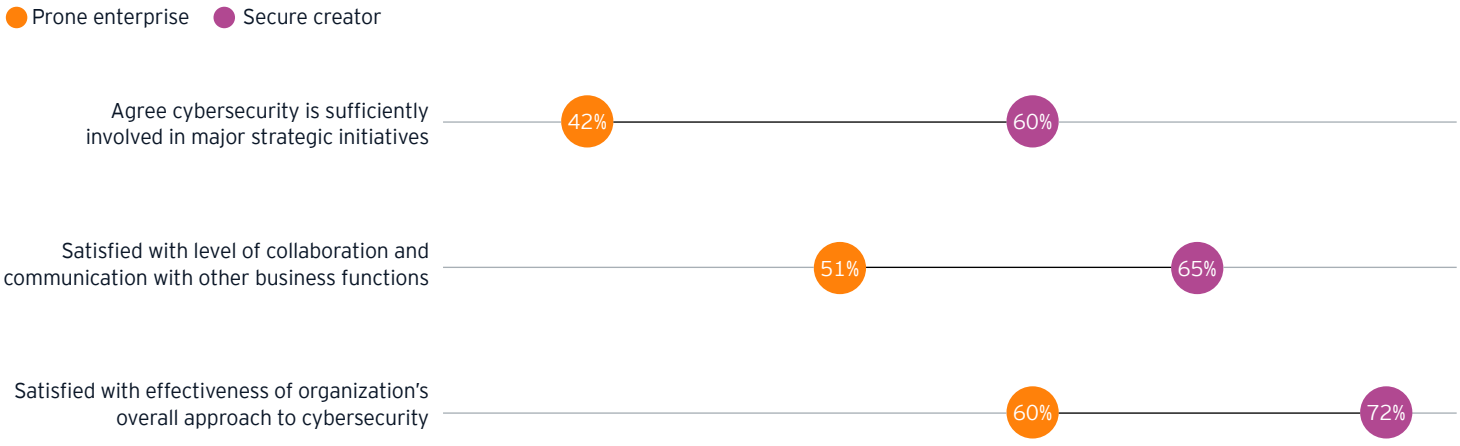
Elevating GRC: From a Tactical Compliance Focus to a Strategic Bridge

To break free from this legacy reputation, GRC must evolve from compliance enforcer to strategic orchestrator. Leaders are redefining GRC with the following attributes:

- **Risk-led:** Align cyber strategy and risk monitoring with enterprise risk appetite. Report on probable loss exposure or revenue at risk — not just operational control counts.
- **Internal unifier:** Convene across cyber domains (cloud, identity, operations, incident response) to establish a collective focus on top risks and an understanding of having the right controls, operating as designed and working together to effectively mitigate risk.
- **Metrics that matter:** Effective cyber risk reporting should align with the organization's risk appetite, support business objectives and enable meaningful oversight at the board level. Rather than relying on a static list of standard security metrics, leading programs define metrics that reflect business impact and strategic relevance. Once these metrics are established, automated dashboards can deliver real-time visibility into cyber posture, spotlighting risk reduction trends and measuring value protection across the enterprise (EY 2025).
- **Data-driven:** Aggregate data feeds from each cyber domain into GRC. Pair this in close partnership with attack and penetration teams to uncover gaps to proactively track remediation efforts ***before attackers do***.
- **Business-facing partner:** Use GRC in partnership with business information security officers (BISOs) as the "face of cyber" to the business, translating technical issues into operational and financial terms.

Increasingly, organizations are exploring how artificial intelligence (AI) can enhance GRC capabilities. Our most recent AI pulse survey reveals that 74% of senior leaders whose organizations are investing in AI are seeing positive ROI from AI in cybersecurity (EY 2025). AI is being applied to support automation of continuous control monitoring, enable predictive risk modeling, and support proactive first- and third-party risk assessments. These innovations help shift GRC from reactive oversight to real-time, intelligence-driven decision support — further aligning cybersecurity with business strategy.

Secure creators approach to cybersecurity helps drive value creation



[Chart 3: Secure creators vs. prone enterprises — showing GRC maturity impact] Source: 2025 EY Global Cybersecurity Leadership Insights Study

What Good Looks Like: Maturity Markers

Organizations that are successfully elevating GRC share common traits:

- **Board and executive-level dashboards** tie cyber risk to enterprise risk appetite.
- **Real-time integration of business contextual data**, threat intelligence and security telemetry exists.
- **Scenario-based exercises** coordinated by GRC include red team testing across people, process and technology — not just detection but also initial response, triage, containment, investigation and crisis coordination. These exercises validate the organization's ability to respond effectively to real-world threats.
- **Risk governance committees** engage the business and align security priorities in the context of business objectives and priorities.
- **Exception and acceptance handling is integrated into GRC** to assess enterprise-level risk exposure — not just application- or control-specific exceptions. This helps prevent fragmented exception processes, especially within engineering functions, that can increase systemic cyber risk.
- **A clear value story that measures loss avoidances and resilience gains** is conveyed across the organization.

These maturity markers make GRC not just a compliance office but also the central nervous system of cybersecurity risk management — providing intelligence, orchestration and strategic foresight.

Conclusion: Turning GRC into a Competitive Differentiator

The Cyber GRC gap is one of the most significant barriers to demonstrating security's value to the business. Left in its traditional role, GRC reinforces silos and slows progress. Elevated, it becomes the bridge between cybersecurity and the enterprise — integrating cybersecurity data across domains, collaborating with attack teams to validate and stay ahead of threats, and translating control and telemetry data into business impact. Organizations that achieve this shift will reposition the cybersecurity function from a cost of compliance function to one that serves as a competitive differentiator built on trust, resilience and growth.

Special thanks to Brian DePersiis, Saverio Ortizzo, Darren DeGroot, Kyle Brunell, Brandon Bapst, Pengfei Wang, Gabby Knight and Arjun Antony for contributions to this content.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

2511-10581-CS
ED None

US SCORE no. 29341-251US

ey.com