Building Next-Gen GRC Programs for Success

The Evolving Role of Governance, Risk, and Compliance (GRC)

Traditionally, GRC and Cybersecurity teams have been viewed as gatekeepers, focused simply on identifying and remediating IT risks. However, as the threat landscape grows more ever-more complex and insidious, directly threatening care operations and patient safety, leading healthcare organizations are shifting this perspective on GRC's role.

'Next-generation' GRC and Cybersecurity professionals now play a pivotal role in guiding executive decisions, helping non-technical leaders and the Board understand and set appropriate risk tolerance levels, and working with the frontline business to decide which risks should be remediated, mitigated, or even accepted. This business-focused approach ensures risk decisions directly support the organization's broader strategy, and helps create a more effective culture of Cybersecurity and Risk throughout the organization based on stronger collaboration, awareness, and accountability.

Below are 4 best practices for building and running a successful GRC program:

1. Set Enterprise Risk Appetite with the Business

One of the hallmarks of a successful GRC program is that the risks carried by the organization are defined and supported by the *business* – not just by IT/Security teams or the Board. As such, GRC leaders ensure that business stakeholders are directly involved in setting and updating the risk appetite across the organization. Key questions for the business, Board, and GRC to consider include:

- What is our organization's overall risk appetite?
- What risks to the business are we willing to accept?
- How do risk tolerances change by business unit or use case?

Creating a regular cadence for discussion is critical as responses to these questions will change as the business grows, new use cases are identified, and threats evolve.

2. Align on Core "Risk Themes" with the Board

Communicating risk effectively requires simplification and clarity, particularly with the Board and non-technical executives. As such, the top GRC leaders communicate risks in the context of potential impact to top-level enterprise priorities – or "risk themes" – like Patient Safety, Financial Wellness, or Strategic Growth. For instance, discussing a specific cyber threat's potential impact on performing safe, high quality procedures in the Heart Center can resonate more effectively than detailing a bad actor's tactics, techniques, and procedures (TTPs).

This helps to connect risk with the business, makes complex issues more accessible and relatable, and enables Board members and GRC leaders to work together to prioritize investment, resources, or take immediate action.

3. Use a Risk Register in the Right Way

Risk registers can be effective tools in managing risk, but too often they become static, unwieldy spreadsheets that are hard to understand, update, or drive accountability. Leveraging a risk register the right way begins with automation, and eliminating all the manual labor associated with managing third-party and enterprise risk. More than just a list of threats, a risk register is a strategic tool for informed, risk-based decision-making. By cataloging and assigning all open risks in a centralized place – including their potential impact, likelihood, disposition, and status – a risk register helps prioritize resources and ensures all risks are resolved or accepted in a timely manner.

A best-in-class risk register is comprehensive yet simple, conveying risks succinctly in business terms and in the context of the organization's risk themes (see above #2). In addition, a risk register should drive accountability and awareness by enabling each risk item or action to be assigned to both a technical owner and a business owner, where applicable.

4. Benchmark Program Performance Against Peers

Peer benchmarking is an invaluable tool for evaluating and improving an organization's GRC program. Comparing program maturity and performance against peers in the context of key performance indicators and 'recognized security practices' like NIST Cybersecurity Framework or 405(d) Health Industry Cybersecurity Practices (HICP) provides both key strategic and tactical insights, including:

- Are we over-investing or under-investing in key areas? Where?
- Are we more or less cost-effective than peer programs? Why?
- Can we justify additional FTEs or investment to the Board?

About Censinet

Censinet is an American Hospital Association Preferred Cybersecurity Provider and is purpose-built to help healthcare organizations assess, manage, and mitigate third-party and enterprise risk.

If you're interested in learning more about how Censinet can help improve your GRC, Cybersecurity, and Risk Management programs, contact us at info@censinet.com or visit https://www.censinet.com

Censinet is an American Hospital Association Preferred Cybersecurity Service Provider for Cyber Firm Risk Management and Information Governance and Cyber Risk Assessment, Privacy and HIPAA Compliance.