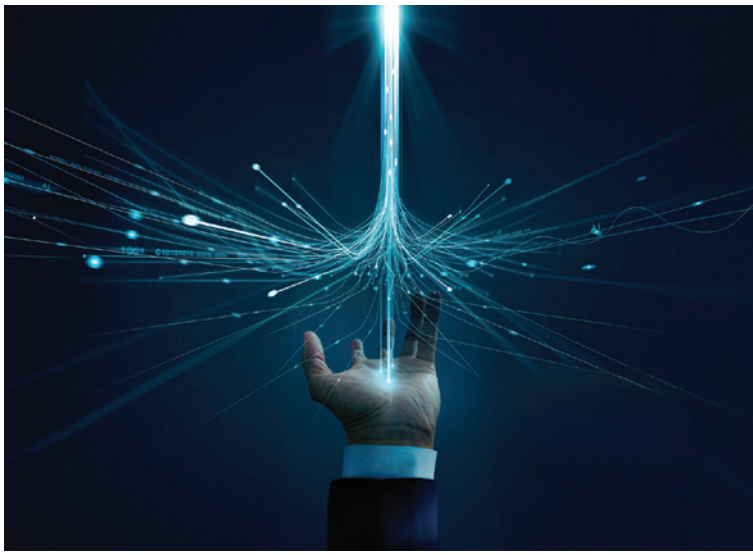
A New Era: Embracing the Role of Digital Risk & Resilience



In the rapidly evolving landscape of governance, risk management, and compliance (GRC), information security is undergoing a significant transformation. This evolution reflects the growing complexity and interconnectedness of digital risks that organizations face today. As businesses become increasingly reliant on digital technologies, the traditional responsibilities of the CISO are expanding, giving rise to digital risk and resilience management.

The Traditional CISO: A Foundation in Security

The CISO role was born out of the need to protect organizational assets in a digital world. The primary mission was clear: safeguard the confidentiality, integrity, and availability of information systems against cyber threats. This role has been crucial in implementing security measures such as firewalls, intrusion detection systems, and data encryption to defend against potential breaches. Over time, the CISO's responsibilities expanded to include compliance with regulatory requirements, vendor risk management, and data privacy.

However, as the digital landscape has grown more complex, so too have the risks that organizations face. IT security is no longer just about preventing data breaches; it now encompasses a broader spectrum of risks, including IT resilience, business continuity, and the ability to recover from disruptions. The CISO role, and with that information security, while essential, needs to expand to address the full range of digital risks that organizations must navigate.

A New Landscape: The Need for Broader Risk & Resilience Management

Today's digital environment is characterized by its interconnectedness and complexity. Risks are no longer confined to isolated incidents; they span across the entire organization, affecting everything from supply chain operations to business continuity. The recent CrowdStrike incident, where a critical vendor's operational disruption impacted multiple organizations, underscores the need for a more comprehensive approach to digital risk management.

Regulatory requirements further complicate this landscape. Regulations such as the EU Digital Operational Resilience Act (DORA), EU Cyber Resilience Act, UK Operational Resilience, and Australia CPS 230 are pushing organizations to adopt a more holistic and integrated view of risk and resilience.

The Evolution: From Information Security to Digital Risk & Resilience

In response to these challenges, the role of the CISO is evolving to include digital risk and resilience management. This expanded role reflects the need for a broader, more integrated approach to digital risk management. The digital risk and resilience role is not just a guardian of security but a strategist responsible for ensuring the organization's overall resilience in the face of the array of digital risks, not just security risks.

This evolving role needs to develop and implement a comprehensive risk management framework that addresses the full spectrum of digital risks, including cybersecurity, IT resilience, business resilience continuity, and compliance. This holistic approach ensures that the organization is not only protected from cyber threats but also prepared to recover quickly from any disruptions that may occur.

The Pillars of Digital Risk & Resilience

1. **Holistic Risk & Resilience Management.** The organization must develop a risk and resilience management strategy that addresses a wide range of digital risks, from cyber threats to operational disruptions. This strategy should include regular risk assessments, scenario planning, and the implementation of robust mitigation measures.

2. **Digital Operational Resilience.** Ensuring that the organization can quickly recover from disruptions is a key focus of digital risk and resilience. This involves creating well-defined recovery plans, conducting regular resilience testing, and continuously improving the organization's ability to respond to and recover from incidents.

3. **Integration of IT and Business Strategies.** Digital risk and resilience play a crucial role in aligning digital risk management with the organization's overall business objectives. By integrating digital resilience and risk management into the broader business strategy, it helps ensure that digital risks are managed in a way that supports long-term growth and resilience.

4. **Proactive Scenario and Risk Intelligence.** Leveraging scenario analysis, tabletop exercise, and advanced risk intelligence, the organization stays ahead of emerging risks by continuously monitoring the digital threat and risk landscape and adapting strategies to address developing risk exposures. This proactive approach is essential in managing the dynamic and ever-changing nature of digital risks.

5. **Stakeholder Collaboration.** Effective digital risk management requires collaboration across the organization. The CISO with a focus on digital risk and resilience works closely with executive leadership, IT teams, business units, and external partners to foster a culture of resilience and shared responsibility.

A Unified Approach to Digital Risk & Resilience Management

As the role of the CISO continues to evolve, it is essential for organizations to adopt a federated approach to risk and resilience management. This strategy involves creating a unified framework that spans across all departments and functions responsible for managing digital risks and business operations, services, and processes. By establishing structured processes organizations can ensure a comprehensive and consistent approach to managing risks.

This unified approach is supported by risk and resilience management technologies and real-time risk intelligence feeds. Additionally, artificial intelligence plays a critical role in automating processes and providing deeper insights into risk scenarios and their impact on the business.

Conclusion: Embracing the Future of Risk & Resilience Management

The evolution from CISO to include digital risk and resilience represents a natural progression in the way organizations approach digital risk management. As businesses navigate the complexities of the modern digital landscape, this role will play a pivotal role in ensuring that they are not only protected from cyber threats but also resilient in the face of disruptions.

This new role reflects a broader, more integrated approach to risk management—one that aligns with the organization's strategic objectives and supports long-term success. By embracing this evolution, organizations can ensure they are prepared to meet the challenges of the digital age with confidence and resilience.

For more on GRC, check out Riskonnect's ***Technology Risk Management software*** *solution.*

10.24

ABOUT RISKONNECT

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents partner with Riskonnect to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia.

Visit riskonnect.com to learn more – or schedule a meeting with our experts here.

CONNECT NOW →

RISKONNECT'S INTEGRATED RISK MANAGEMENT SOLUTIONS

- **Risk Management Information System**
- **Claims Administration**
- **Billing**
- **Policy Administration**
- **Third-Party Risk Management**
- **Enterprise Risk Management**
- **Environmental, Social, Governance**
- **Business Continuity & Resilience**
- **Internal Controls Management**
- **Compliance**
- **Internal Audit**
- **Policy Management**
- **Project Risk Management**
- **Technology Risk Management**
- **Active Risk Manager**
- **Business Strategy**
- **Health & Safety**
- **Healthcare**

riskonnect