IS IT TIME FOR A CHECK-UP?

Organizations are subject to increasing amounts of legislative, corporate and regulatory requirements to show they're managing and protecting their information assets appropriately.

As the threats from cyber criminals and hacktivists grow in scale and sophistication, how can businesses assess the maturity of their risk management mechanisms, against the backdrop of a mercurial security landscape, to reassure employees, customers and stakeholders that appropriate safeguards are in place to protect their information assets and to defend against cyber-attacks?

Do you comply with the varied regulatory requirements?

There is a significant responsibility on executives to understand security vulnerabilities and demonstrate corporate and operational compliance with various regulatory requirements.

STRATIUUM's Compliance Health Check is a high-level evaluation of the key elements of your cybersecurity program, tailored specifically to the capabilities identified in relevant regulatory and legal requirements, specific to your organization.

We leverage our Cyber Security Maturity Assessment methodology which incorporates our knowledge of the cyber risk landscape, our experience assessing cyber capabilities, and our extensive expertise evaluating cyber security programs.

Health Check benefits

In addition to providing an objective and independent view of your organization's ability to comply with current and upcoming requirements, STRATIUUM's Compliance Health Check can:

- ✓ Equip you with valuable insights into how efficiently you are managing cyber risks
- ✓ Help you optimize and prioritize your cybersecurity efforts
- ✓ Guide risk mitigation activities and future investments in cybersecurity
- ✓ Enhance your leadership teams' awareness of their cybersecurity fiduciary and regulatory obligations

OUR APPROACH

Our experienced advisers evaluate your current cyber capabilities across multiple dimensions including governance and strategy, security defenses and controls, threat and vulnerability management, and incident readiness, response, and resilience.

We implement a phased approach to identify the true nature of your organization's threat profile, assess your cybersecurity posture, compare your capabilities to the relevant regulatory and legal requirements, and provide practical and actionable recommendations to assist you in maturing your organization's cybersecurity program.

01

BUSINESS PROFILE AND PLANNING

Establish overall business context and determine threat profile based on business model, mission, and strategy

CURRENT STATE ASSESSMENT

02

Understand current cybersecurity posture in order to establish a baseline for future improvements

03

ACTIONABLE RECOMMENDATIONS

identify practical and actionable recommendations to improve cyber security posture and regulatory compliance

DELIVERY AND SOCIALIZATION

04

Prepare relevant stakeholders to execute on their internal and external reporting and certification requirements

The path to a more mature cybersecurity posture

BUSINESS PROFILE AND PLANNING

This phase consists of preparation and planning activities to agree the assessment scope and timeline, identify relevant documentation for review, and engage key stakeholders. We undertake a limited risk assessment to understand the "crown jewels" that support your business model and strategy, and identify threat actors and threat techniques most relevant to your organization.

Armed with this information, we can identify and prioritize the cyber capabilities that will contribute most to improving your organization's overall cyber resilience.

CURRENT STATE ASSESSMENT

Next, our advisers review relevant cybersecurity program documentation and meet with applicable stakeholders to understand your current cybersecurity posture.

Understanding the current state of your organization's cyber capabilities provides a baseline from which we can ascertain any compliance gaps or weaknesses, and identify future improvements or mitigation strategies.

ACTIONABLE RECOMMENDATIONS

Following completion of the current state review, we evaluate your cyber capabilities across multiple dimensions in the context of leading industry practices and peer organizations. Observations and findings are documented, along with actionable recommendations to help improve your organization's overall cyber security posture and facilitate regulatory compliance.

DELIVERY AND SOCIALIZTION

To prepare relevant stakeholders to execute on their internal and external reporting obligations as they relate to your firm's cybersecurity program, our advisers provide an onsite presentation to your leadership team, where we explain our findings and recommendations, and answer questions related to the assessment.

6 to 11 WEEKS

ESTIMATED TIME TO COMPLETE

OUR CYBER RISK MATURITY ASSESSMENT DIMENSIONS

To truly understand the effectiveness of your cyber risk program, we evaluate your current cyber capabilities across multiple dimensions, taking into consideration leading industry practices along with insights gained from delivering cyber strategy engagements for peer organizations.

STRATEGY AND GOVERNANCE

Embedding the necessary structures and risk framework to maintain and enhance cybersecurity capabilities, aligned to the organization's strategic objectives and goals

- Cybersecurity strategy, roadmap, and investments
- Policies, standards, and procedures
- Cyber risk management, metrics, and reporting
- People, resources, and training

SECURITY DEFENSES AND CONTROLS

Risk-based, proactive approach to identify, implement, and enhance key cybersecurity controls

- Asset management
- User access controls
- Systems and network security
- Data loss prevention
- Encryption
- Third-party risk management

THREAT AND VULNERABILITY MANAGEMENT

Situational awareness to anticipate, discover, and avert internal and external threats

- Threat intelligence and industry specific insights
- Penetration testing and vulnerability scanning
- Systems and network monitoring
- Brand protection

INCIDENT READINESS, RESPONSE, AND RESILIENCE

Ability to recover from, and minimize any adverse impact to the organization from, cyber security events

- Incident management framework, processes, and playbooks
- Incident response plans
- Breach notifications
- Communication strategy and protocols

Would you spend $10 Million to avoid a $1 million loss?

In an age of competing priorities and limited resources, it would be wholly impracticable to apply the Cheney doctrine – if there is 1% chance of something occurring, you must deploy 100% of your resources to prevent it – to the cyber threat landscape.

Firms have to prioritize their cyber risk efforts to maximize the return on their cybersecurity investments.

Are you ready to attest to your firm's compliance?

As the spotlight on cyber continues to intensify with increasing demands and scrutiny from a variety of stakeholders – institutional investors, activists, the media, regulators, and customers - STRATIUUM's Compliance Health Check can help you discern the true nature of your organization's threats and vulnerabilities, setting you up to manage cyber risk proactively, comprehensively, and effectively.

CONTACT

To learn more about STRATIUUM's cybersecurity Compliance Health Check or Cyber Resilience Solutions, please contact:

Cath Stewart
Managing Principal
New York, NY

cstewart@stratiuum.com

About STRATIUUM

We are a specialized risk advisory firm built to help clients navigate today's complex operating environment and turn their most critical business challenges into sources of strategic opportunity. Our focus is on emerging strategic risks that pose serious threats to an organization's bottom line, growth prospects and market standing. Against the backdrop of today's nefarious threat landscape, we help our clients identify and protect their organization's critical assets, reduce the impact of a cyber event and align security investments with risk priorities. For more information about our organization and solutions, please visit **stratiuum.com**
