WHITE PAPER

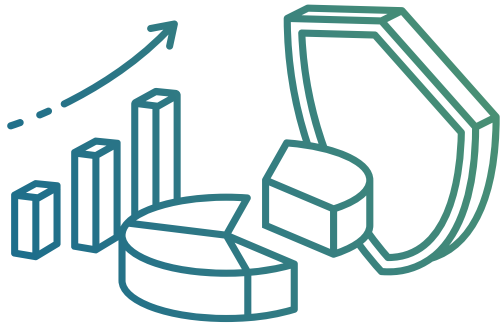
Achieving New SEC Cybersecurity Compliance Through Proactive Risk Management

What your company needs to do right now.

The new SEC compliance regulations require organizations to have processes to assess, identify, and manage cybersecurity risks, as well as report material incidents quickly. To do this effectively, cybersecurity efforts must be aligned with business strategy, and a comprehensive approach to risk management is necessary to avert the consequences of non-compliance.

NEW STRICTER SEC GUIDANCE

SEC regulations regularly change to protect organizations as cybersecurity threats evolve and grow. The new and preexisting rules are designed to better inform investors about a registrant's risk management, security strategy, and governance; additionally, the rules dictate timely notification of material cybersecurity incidents. Consistent, comparable, and decision-useful disclosures allow investors to evaluate their exposure to cybersecurity risks and incidents and enable them to manage and mitigate those risks in relation to their shareholder value.



The disclosure facets that the SEC mandates are part of the overall process, and while they can appear daunting because they touch all aspects of an organization, regulatory responsibilities can be met with the correct guidance and accountability.

Some aspects of the *new SEC rules* include:

- *Materiality Assessment:* The SEC emphasizes the importance of organizations developing a comprehensive impact assessment of cybersecurity risks and incidents. This assessment should consider both quantitative and qualitative factors when evaluating the material impact of events on their operations, financial condition, and reputation.

  Disclosure is required within four business days from the date the incident is considered material. A cybersecurity incident is considered "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."

- *Renewed Focus on Processes:* The new ruling moves the focus away from disclosure of specific policies and procedures related to risk management, strategy, and governance. Instead, it pushes for a comprehensive disclosure of processes.

  This rule necessitates disclosure of any information available that could affect investors' decisions, including disclosure of the risks associated with cybersecurity threats, their potential impact on the company's operations, and steps taken to mitigate these risks. Disclosure requirements include, but are not limited to:

  - The cybersecurity processes that have or have not been integrated into the organization's overall risk management strategy.

- Details on whether the organization utilizes consultants, auditors, or other third parties in its security processes.
- The processes the organization has in place to oversee and identify material risks from cybersecurity threats associated with its third-party service providers.

- *Governance:* The SEC expects disclosure of cybersecurity governance from the board of directors and leadership with specifics on how they oversee cybersecurity processes. Full disclosure of the board's oversight of cybersecurity risks, the board members responsible for the oversight, and the process involved in communicating risks are all designed to allow key stakeholders and investors insight into how the organization manages its risk.

Implementing systematic, proactive risk management processes that address these challenges and weaving them into the fiber of the organization's overall business strategy creates a protective barrier between the organization and compliance failure.

CHALLENGES: Understanding the Challenges of the SEC Changes

To effectively address the new SEC rules, organizations need to work quickly to align their cybersecurity efforts with their broader business strategy. Current methods often fall short for a variety of reasons unique to each organization; however, here are the most common challenges:

Inability to Make Informed Decisions: Organizations that cannot quantify their risks efficiently or that fail to have a thorough understanding of their resources cannot make quick, well-informed security decisions that support their overall business strategy and effectively protect their organization's assets. In the past, organizations may have gotten by with making decisions on the fly, but the new SEC regulations will require more diligence. Quantifying risks and understanding resources typically requires experienced staff and a comprehensive approach – two things many organizations don't have.

Morphing Mandates: The SEC regulations are an example of the constantly changing regulatory landscape. Navigating this dynamic environment requires a commitment to actively monitoring, managing, and maintaining risk. Too often, the day-to-day challenges of business monopolize an organization's attention, often at the expense of staying on top of critical regulatory changes. By prioritizing consistent reviews of compliance standards and regulation changes, valuable trust is built among customers, partners, employees, and investors.

Poor Communication: According to a recent ***Gartner report***, "human failure" will be responsible for over half of all major cyber incidents over the next three years. Poor communication remains one of the greatest cybersecurity threats to an organization. Building organizational discipline and support pertaining to cybersecurity without clear communication is a proven recipe for non-compliance and the human failure element.

Shared understanding and consistent communication both mitigate risk and work to maintain compliance. This certainly requires seamless communication between team members but also necessitates devoted time and resources from the organization's board, management, and stakeholders.

Inconsistent Risk Management: Many organizations fail to monitor their threat landscape consistently and continuously, leaving them vulnerable to emerging risks. Inconsistency compromises the ability to respond rapidly to potential incidents. By integrating cybersecurity processes into the organization's business strategy along with a timeline for implementation of security controls, detection systems, and incident response mechanisms, organizations can build cyber resilience, minimize cyber threats, and reduce their potential to disrupt operations.

Insufficient Funding: Failure to prioritize funding for cybersecurity and align it with the broader business strategy can lay an organization vulnerable to cyberattacks and additional costs, which may include:

- **Financial Losses:** Losses from a cyberattack include direct costs of incident response, remediation, and regulatory fines, as well as indirect costs like reputational damage and customer churn.
- **Disruption of Operations:** Disruptions cause downtime, loss of productivity, and delays in delivering products or services to customers; this may lead to revenue loss, customer dissatisfaction, and cost overruns.
- **Damage to Reputation:** Cybersecurity breaches harm an organization's reputation, eroding customer trust and loyalty. Rebuilding a tarnished reputation can be a lengthy and costly process.
- **Legal and Compliance Risks:** Non-compliance with cybersecurity regulations can result in legal and financial risks, including penalties, lawsuits, and regulatory scrutiny, further damaging an organization's reputation and financial stability.
- **Loss of Competitive Advantage:** Customers and partners increasingly prioritize secure and trustworthy organizations in today's digital landscape. Align cybersecurity with business strategy to avoid a loss of competitive advantage, as customers may choose more secure alternatives.

IBM Security reported that the average cost of a data breach reached a record high in 2022 with the global average total cost at $4.35 million. Very few organizations can afford to not properly fund risk management initiatives.

THE SOLUTION: The Best SEC Defense is an Offensive Cybersecurity Strategy

For organizations to meet SEC cybersecurity requirements, they need to take an offensive approach to their security by establishing a baseline strategy that defines the integration and automation of detection and response processes; and operationalizes a comprehensive, ongoing reporting framework.

Establishing a cybersecurity baseline involves assessing the organization's current security situation, identifying vulnerabilities and risks, and implementing mitigation measures.

A baseline, offensive project would include:

Defining the Scope: Determine the scope of the evaluation, including the systems, networks, applications, and data in the assessment.

Identify Relevant Standards and Regulations: Understand the applicable cybersecurity standards, regulations, and frameworks your organization should adhere to, such as *ISO 27001*, *NIST Cybersecurity Framework*, or industry-specific requirements.

Conduct a Risk Assessment: Perform a comprehensive risk assessment to identify potential threats and vulnerabilities, as well as their potential to impact your organization. This assessment can include technical vulnerabilities, physical security risks, and human factors.

Review Existing Policies and Procedures: Evaluate your organization's security policies, procedures, and guidelines. Identify any gaps or areas that need improvement and update them accordingly.

Assess Security Controls: Review and assess the effectiveness of your organization's current security controls, such as firewalls, intrusion detection systems, antivirus software, access controls, and encryption mechanisms.

Perform Vulnerability Assessments: Conduct vulnerability assessments and penetration tests to identify weaknesses in your systems and networks. This process helps uncover potential entry points for attackers and reveals vulnerabilities that may be exploited.

Evaluate Security Awareness and Training: Assess your organization's security awareness and training level. Evaluate whether employees know cybersecurity best practices and whether training programs are effective.

Review Incident Response Plans: Evaluate your organization's incident response plans to ensure they are comprehensive and current. Assess your organization's preparedness to detect, respond, and recover from cybersecurity incidents.

Analyze Network and System Logs: Review network and system logs to identify unusual or suspicious activities. This analysis can help detect potential security breaches or unauthorized access attempts.

Engage External Experts: Consider engaging external cybersecurity experts or conducting third-party audits to gain an unbiased assessment of your organization's security baseline. SDG is a trusted and experienced partner in this domain.

Document Findings and Recommendations: Document all findings, vulnerabilities, and recommendations in a detailed report. Include prioritized remediation actions to address identified risks and vulnerabilities.

Implement Remediation Measures: Prioritize and implement the recommended remediation actions based on their criticality and potential impact on your organization's security posture.

Regularly Monitor and Update: Establish a process for ongoing monitoring, assessment, and updating of your organization's security baseline. Cybersecurity is a continuing process; regular evaluations are crucial to maintaining a strong security posture.

Cybersecurity evaluation and adaptation should be continuous to keep pace with evolving threats and new technologies. Regular reassessment and updating of your organization's security baseline ensure its effectiveness.

CONTINUOUS MONITORING AND PROACTIVE RISK MANAGEMENT:
Staying Ahead of Evolving Threats

Continuous monitoring as a proactive risk management approach is highly effective for staying ahead of evolving threats. Early planning and adaptation of tailored roadmaps afford organizations the luxury of preemptively addressing risk and resolving the issue before anything sinister can occur. Continuous monitoring in cybersecurity involves:

Real-Time Data Collection from various sources such as network logs, system logs, security sensors, and other relevant systems provides valuable insights into the organization's operations, potential vulnerabilities, and emerging risks.

Automated Event and Log Analysis utilizing automated tools and technologies to analyze the collected data for anomalies, trends, and potential risks can help promptly identify security breaches, suspicious activities, and non-compliant behaviors.

Risk Assessment and Prioritization involves assessing and prioritizing risks based on their potential impact on the organization's objectives and assets. This process helps allocate appropriate resources and attention to the most critical threats.

Incident Detection and Response enables the early detection of security incidents or breaches by promptly identifying deviations from established patterns or normal behaviors. It facilitates the timely response to incidents, reducing potential damage and minimizing downtime.

Compliance Monitoring helps ensure compliance with regulatory requirements, industry standards, and internal policies. Organizations can identify gaps and take necessary actions to address non-compliance issues through regular assessments.

Vulnerability Management includes regular vulnerability assessments and scanning to identify weaknesses in the organization's infrastructure, systems, and applications. This allows for proactive remediation and patching to reduce the risk of exploitation.

Threat Intelligence Integration incorporates external threat intelligence sources to stay updated on emerging threats, attack vectors, and new vulnerabilities. By integrating this intelligence, organizations can proactively adapt their security measures to counter evolving risks.

Reporting and Communication requires effective mechanisms be in place to ensure that risk-related information reaches the relevant stakeholders. This enables informed decision-making, timely remediation, and ongoing risk mitigation.

Constant Improvement: Continuous monitoring is not a one-time activity but an iterative process. It involves regularly reviewing and refining monitoring strategies, technologies, and methodologies to enhance risk detection and response capabilities over time.

By considering these elements, organizations can establish a robust and proactive monitoring approach that allows them to effectively identify, assess, and mitigate risks, thereby enhancing their overall security posture.

QUANTIFYING CYBERSECURITY RISKS FOR INFORMED DECISION-MAKING

To optimize security investments and minimize financial exposure, organizations must move from just reporting on risks to quantifying risks. Quantifying risks necessitates assessing, measuring, and analyzing all risk factors. In doing so, organizations become well-informed of their security posture, allowing for swift, accurate decisions.

PARTNERING WITH AN ESTABLISHED AND EXPERIENCED CYBERSECURITY PARTNER THAT KEEPS YOU AHEAD OF RISKS AND REGULATIONS

Finding a trusted partner who has extensive experience with private and public companies across multiple industries is critical to staying ahead of risk and compliance.

SDG, a global provider of cybersecurity, identity, risk, compliance, and cloud security technology, has over 30 years of experience providing managed services and consulting with organizations on achieving SEC compliance through proactive risk management. The SDG approach emphasizes an organization's overall cybersecurity posture and specializes in utilizing legacy and innovative cybersecurity solutions to achieve proven results.

SDG'S STRUCTURED APPROACH TO RISK

SDG adheres to a structured, comprehensive approach to identifying all aspects of an organization's risk. It involves assessing, measuring, and analyzing various factors of the organization's overall vulnerability and readiness. Here are examples of the exhaustive steps SDG takes to fully understand an organization's risks before creating a cost-effective, thorough approach to protecting the organization's assets.

Identify Assets: SDG identifies the critical assets needing protection. These assets include data, hardware, software, networks, intellectual property, and more.

Threat Assessment: SDG evaluates all potential threats targeting the identified assets and considers external threats (such as hackers, malware, or data breaches) and internal threats (such as employee errors or malicious insiders).

Vulnerability Assessment: SDG determines the vulnerabilities or weaknesses within the organization's systems and processes that potential threats could exploit. This process could involve conducting security assessments, penetration testing, and reviewing security controls.

Impact Analysis: When assessing the potential impact of a successful cyberattack on the organization, SDG considers financial losses, operational disruptions, reputational damage, legal and regulatory implications, and potential harm to customers or stakeholders.

Likelihood Determination: SDG estimates the likelihood of various threats exploiting vulnerabilities, and it identifies the potential impacts. This estimate may include historical data, threat intelligence, industry benchmarks, expert opinions, and risk modeling techniques.

Risk Calculation: Calculating the risk level by multiplying the impact and likelihood values allows SDG to help your organization prioritize risks and focus on areas that pose the highest risk to the organization.

Risk Mitigation Strategies: SDG identifies and implements appropriate risk mitigation strategies based on your organization's unique calculated risks. These strategies may involve implementing security controls, employee training, incident response planning, regular monitoring, and updating security policies and procedures.

Quantitative Metrics: SDG considers quantitative metrics—the measurement and tracking of cybersecurity risks over time—important to understanding risk. These could include metrics such as the number of security incidents, the average time to detect and respond to incidents, the financial impact of breaches, or the effectiveness of implemented security controls. Quantifying cybersecurity risks is a complex task, and it's important to involve cybersecurity experts like SDG, internal risk managers, and other relevant stakeholders within the organization to ensure a comprehensive and accurate assessment for effective results.

CREATING A CONTINUOUS MONITORING APPROACH FOR PROACTIVE RISK MANAGEMENT

SDG regularly monitors and reassesses cybersecurity risks as threats evolve and new vulnerabilities emerge, allowing organizations to stay updated on the latest industry trends, security best practices, and the emerging technologies required to pivot risk management priorities quickly.

At SDG, continuous monitoring includes tailored roadmap suggestions for cybersecurity improvements. We work with organizations to preemptively address and resolve identified risks so cybersecurity defenses can be fortified before an attack, significantly improving their risk management posture.

SDG'S SIMPLIFIED STAKEHOLDER COMMUNICATION IS CRUCIAL TO CYBER RISK TRANSPARENCY

Managing stakeholder communication can require translating complex cybersecurity processes and technologies into business and financial terms. SDG works to provide stakeholders with a complete view of their organization's overall cybersecurity posture, effectively providing content for board oversight discussions, business strategy alignment, and accurate decision-making.

CONCLUSION

To achieve SEC compliance and implement a proactive risk management approach, organizations must align their cybersecurity efforts with their business strategy. By addressing challenges, quantifying cybersecurity risks, adopting proactive risk management measures, and partnering with a trusted cybersecurity service provider like SDG, **organizations can ensure effective SEC compliance, mitigate risks, and bolster their cybersecurity resilience in an ever-evolving threat landscape**.

ABOUT SDG

SDG is a global cybersecurity, identity governance, risk consulting, and advisory firm that advises and partners with clients to address their complex security, compliance, and technology needs and delivers on strategy, transformation, and long-term management of their cybersecurity and IAM programs.

To learn how SDG can help you ensure the security and compliance of your technology and data infrastructure, visit **SDGC.com** or call us at **+1 203.866.8886**.

SDG

- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com