CrowdStrike Services
Data Sheet

SEC Readiness Services

Risk Management Review and Materiality Exercises

Aligning organizations to the SEC rules on cybersecurity

New rules pose new challenges

The new cybersecurity disclosure rules issued by the U.S. Securities and Exchange Commission (SEC) in July 2023 reflect the agency's clear message that cybersecurity is paramount. Public companies are now required to disclose their processes for assessing, identifying and managing material cybersecurity risks in their annual 10-K filing and also report material cyber incidents within four days of determining the incident is material. Inaccurate or misleading disclosures, even if inadvertent, can result in litigation or enforcement actions. At the heart of many of these actions is a key question:

Are you actually doing what you say you are doing?

Manage cyber risk with confidence

The CrowdStrike Risk Management Review helps build confidence in your organization's treatment of cyber risks by taking a two-pronged approach: A CrowdStrike Technical Assessment provides a bottom-up perspective of key risk factors across the enterprise, while a CrowdStrike Programmatic Assessment takes a top-down view to understand the processes that govern and influence risk management activities.

The Technical Assessment uses the CrowdStrike Falcon® platform to identify internal and external IT configurations that pose potential security risks. Reviewing these risks can help identify areas where your company may not be complying with its own policies, or potentially where your practices do not match your public disclosures. It can also provide early warning about larger problems, such as enforcement gaps or ongoing threat activity.

The Programmatic Assessment uses a pair of interactive workshops to delve into how your company identifies and treats different cyber risks, and the governance structures that support these efforts. This allows CrowdStrike experts to identify areas where your company may be better able to make sure its policies, practices, and disclosure align and mitigate demonstrable risks. The executives responsible for SEC disclosures often include people who are not involved in the day-to-day management of the company's cybersecurity risk program. However, those people should still have confidence that their company's security programs and processes can support their public filings.

Key benefits

Increase confidence in answering the following:

- Do our security processes translate to real risk reduction?
- Do we actually have the security controls we think we do?
- Do our practices match what we disclose?

Key service features

The **Technical Assessment** uses CrowdStrike Falcon® Exposure Management to identify risk factors within the following areas:

Category	Security Control
Accounts	Old Passwords, Cached Credentials, Failed Remote Authentications
Vulnerabilities	US-CERT Top Targeted CVEs, Ransomware-related CVEs, Systems Requiring Reboot
Endpoint Management	OS Hygiene, Falcon Sensor Version Review, Unmanaged Assets, Drive Encryption
Zero Trust	OS Hardening Configuration Review
Applications	End-of-Life Application Review
Active Directory Misconfigurations	Privileged Accounts, Weak Passwords, High Risk Accounts, SPN Review, Kerberos Review

The **Programmatic Assessment** consists of two workshops aimed at addressing the following questions:

Workshop Topic	Key Questions
Strategy and Governance	• How well does the security program align with the business? • How well does the company know its most critical assets? • Is the security organization structured to provide strong oversight and governance? • Does the security strategy align with risk appetite?
Risk and Compliance	• How well are cyber risks integrated into the enterprise risk management process? • How effectively does the company identify, treat and track cyber risks? • Does the company maintain and enforce policies that align with its risk appetite and compliance obligations? • Does the company effectively account for third-party cyber risk?

Materiality Exercises

Exercise your material incident disclosure process with a tabletop exercise. CrowdStrike's team of experts will develop a scenario and facilitate a discussion designed to test the processes you have for reviewing material incidents.

Learn more →

About CrowdStrike Services

CrowdStrike Services delivers Incident Response, Technical Assessments, Training and Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations and recover from a breach with speed and precision. Harnessing the power of the CrowdStrike Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary-focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/services

Email: services@crowdstrike.com

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/