REQUEST FOR COMMENT RESPONSE

Consultation Paper P012-2026: Proposed Amendments to Notices on Technology Risk Management

31 July 2026

I. INTRODUCTION

CrowdStrike welcomes the opportunity to respond to the Monetary Authority of Singapore's ("MAS") *Consultation Paper P012-2026 on Proposed Amendments to Notices on Technology Risk Management* (the "Notice"). We commend MAS for its continued commitment to strengthening the technology resilience of Singapore's financial services sector and for inviting industry input into this process.

We approach these comments as a leading international, U.S.-headquartered, cybersecurity provider that defends enterprises from globally distributed threats. Our AI-powered, cloud-native platform delivers state-of-the-art, real-time detection, automated protection, and threat intelligence across endpoints, cloud, identity, data, and AI workloads. Our insights are informed by applied, real-world experience across global industries through our software-as-a-service cybersecurity platform, incident response, managed threat hunting, and managed security services. CrowdStrike's recommendations are grounded in this operational experience.

CrowdStrike offers the following comments in response to MAS's consultation questions.

II. COMMENTS

Question 1: Scope of the IT Asset Inventory

CrowdStrike supports the proposed requirement for Financial Institutions (FIs) to maintain a comprehensive and up-to-date inventory of IT assets, including hardware, software, cryptographic assets, open-source components, and third-party components. The inclusion of open-source and third-party components in the inventory scope reflects the contemporary threat environment, in which supply chain vulnerabilities represent one of the most consequential and underappreciated attack surfaces facing financial institutions.

Inventories are a useful tool for an organization to capture a snapshot but ultimately are only reflective of a point in time and cannot reflect a real-time measure of the state of an organization's security posture.

CrowdStrike recommends that MAS emphasize in its final notice, or accompanying guidance, that asset inventory maintenance must be a continuous process rather than a periodic exercise. A stale inventory provides false assurance and undermines the downstream risk management processes that depend upon it including vulnerability management, change management, and incident response.

Question 2: Scope of IT Risk Assessment, IT Risk Register, and KRIs
CrowdStrike supports the proposed requirement for FIs to establish and maintain an IT risk assessment framework that accounts for threats to their systems, including AI-enabled threats and supply chain risks. The explicit inclusion of AI-enabled threats in the scope of required IT risk assessments reflects the evolving threat landscape and is consistent with CrowdStrike's own threat intelligence findings.

Including specific Key Risk Indicators (KRIs) into the regulatory text of the Notice risks those metrics becoming outdated as the threat landscape and technology environment evolve. FIs also operate with materially different risk profiles, business models, and technology architectures. A uniform KRI set may be insufficient for some institutions and unnecessarily burdensome for others.

Question 4: Continuous System and Security Monitoring
CrowdStrike supports the proposed requirement for FIs to establish and maintain a framework for continuous monitoring of critical systems. This requirement represents modern, effective cybersecurity practices. MAS's own observation — that a number of major IT incidents could have been averted if FIs had promptly discovered and responded to issues — underscores why detection speed and response integration are not merely best practices but operational necessities.

To achieve the goal of a continuous monitoring framework, organizations should leverage several key technologies to defend against cyber threat actors:

- **Cloud Security**: Leveraging cloud systems provides numerous operational efficiencies and security enhancements. Given today's rapidly evolving threat landscape, organizations must address cloud-specific and cross-domain threats (where adversaries traverse cloud and on-premise environments).

Security teams must protect data, manage identity and access, and hunt for and respond to threats in real-time. Capabilities of particular relevance include cloud workload protection, cloud-native application protection platform (CNAPP), cloud security posture management (CSPM), and Software-as-a-Service (SaaS) security.

- **Endpoint Detection and Response (EDR)**: EDR solutions defend endpoints such as desktops, laptops, servers, mobile devices, and cloud workloads from malicious activity. EDR provides granular visibility of potential threats. This enables holistic, real-time threat detection and proactive threat prevention. Leveraging EDR, defenders can perform threat hunting, incident response, and a variety of other essential cybersecurity tasks. EDR capabilities are a core pillar of most contemporary sophisticated security programs.

- **Next-Generation Security Information and Event Management (SIEM) solutions:** Sophisticated threats mean that modern enterprises must achieve visibility, context, and protection across systems and resources, including cloud and ephemeral resources. This often implies the need for multiple security and monitoring tools or capabilities. Next-Gen SIEM solutions leverage rich endpoint telemetry (like that captured by Endpoint Detection and Response [EDR] tools) and integrate it with other security-relevant event information from an array of sources. Supported by AI, this provides defenders a more coherent view, intuitive workflows, and ultimately better control of their environments.

- **Artificial Intelligence-Based Prevention**: The core of modern cybersecurity solutions is the ability to prevent zero-day attacks and malware-free attacks, and achieve visibility across environments. Machine learning and artificial intelligence are essential to this end. Leveraging these technologies is essential to meeting constantly-evolving threats.

- **AI Detection and Response (AIDR)**: Security teams increasingly require specialized capabilities to protect the enterprise throughout the AI lifecycle. An emerging security category called AIDR enables security teams to: monitor AI behavior and interactions; secure AI agent identities and access; discover shadow AI; prevent sensitive data leakage to AI systems; protect cloud-based AI applications; and implement guardrails on AI system actions.

- **Identity Threat Detection and Response (ITDR)**: As organizations increase deployment of cloud services, work from anywhere models, and Bring-Your-Own-Device policies, enterprise boundaries continue to erode. Threat actors exploit resulting gaps and weaknesses from traditional authentication methods. In fact, compromised valid identities are a common initial access vector in incidents. However, emerging identity-centric approaches to security defeat these threats using a combination of real-time authentication traffic analysis, telemetry from endpoints, and machine learning analytics to quickly identify and prevent identity-based attacks.

Additionally, there are multiple security program requirements that bolster organizations' security posture:

- **Threat Hunting**: Whether through supply chain attacks or otherwise, adversaries periodically breach even very-well defended enterprises. However, skilled defenders can find them and thwart their goals. Proactive hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. The more well-instrumented the environment, the more opportunities defenders give themselves to identify malicious activity as an attack progresses through phases. Optimally defenders or their service providers continually hunt for threat activity 24/7, 365 days per year.

- **Zero Trust Architecture:** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate security protections focused on identity and authentication. By eliminating transitive trust, Zero Trust Architecture concepts radically reduce or prevent lateral movement and privilege escalation during a compromise. This constrains threat actors' ability to achieve actions on objective and provides additional opportunities for defenders to detect threats.

- **Logging Practices**: Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

- **Managed Security Service Providers**: Some entities lack the cybersecurity maturity to run effective security programs internally, or lack the scale to support a robust, 24/7, 365 days per year security capability. Increasingly, such entities should rely upon managed service providers, which can be more efficient overall and enable organizations to apply internal IT/security resources toward domain-specific challenges, including governance, risk, and compliance. Adopting an MSSP can radically strengthen organizations' security posture.

Question 7: Incident Management Framework

Definition of Cybersecurity Incident

CrowdStrike encourages MAS to consider achieving balance in defining "cybersecurity incident." The volume of resulting reports should be sufficient to discover and alert entities about systemic and/or widespread threats; but not be so great as to create "noise" for analysts and extra work for those affected by low-impact commodity threat activity.

In cybersecurity, an important distinction exists between alerts and incidents, which should help inform notification scenarios and regulations. In most cases, organizations using contemporary cybersecurity solutions are alerted to malicious activity occurring in their environment. The nature of these alerts may vary, and could cover something like the installation of malicious software on one system, or the compromise of a single account. In scenarios where defenders see these alerts and address them quickly, the alert may not rise to the threshold of a cybersecurity "incident," where the threat actor has not meaningfully achieved their objective, accessed sensitive information, and the like.

The attack vector alone should not be a predicate for a covered incident; the outcome of the attack (e.g., a material impact) should determine reportability regardless of the means. This approach ensures the definition remains durable as adversary tactics, techniques, and procedures evolve over time.

Incident Reporting Timeline

CrowdStrike encourages MAS to reconsider the requirement that entities report cybersecurity incidents to MAS upon discovery within 1-hour. Based on our experience performing incident response services for a variety of cyberattack victims, entities confront significant constraints in the immediate hours of an incident. In some cases,

satisfying reporting obligations may divert resources and attention from the incident remediation process itself. This, in turn, could amplify the impact of the incident.

A 72-hour initial reporting window is rapidly emerging as the common international timeframe, reflected in frameworks such as the European Union's NIS2 Directive and the U.S. Cyber Incident Reporting for Critical Infrastructure Act. Rather than requiring immediate reporting, CrowdStrike recommends MAS adopt this 72-hour standard for an initial notification, with supplemental and final reports submitted as the investigation matures and additional facts become available.

Notably, incidents with divergent impacts could look similar in the early investigation stage. Requiring immediate reporting before an entity has had adequate time to assess the nature and scope of an intrusion will result in the submission of incomplete, extraneous, or potentially inaccurate information. A 72-hour window allows entities to conduct necessary triage while still ensuring MAS receives timely notification of significant events.

III. CONCLUSION

MAS's proposed Notice represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. Generally speaking, the financial sector uses strong cybersecurity practices due to the amount of sensitive data they protect and the regulations to which they are subject. With an emphasis on adoption of practical security practices, these new requirements can raise the already high standard of cybersecurity in the financial sector. As MAS moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any proposed updates focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving

adversary tradecraft, and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting, and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity, and immediate time-to-value.

CrowdStrike: We stop breaches.

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

CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley
Chief Privacy and Policy Officer

Brian Fletcher
Director Public Policy APJ

Email: policy@crowdstrike.com

***