A24 Limited
[redacted]

Release 1

A24 Limited

Project Team

Shane Tully – Global Chief Information Security Officer
Szeern (Zee) Wong – Sales & Talent

May 2023

Table of Contents

1 A24 Recommendations for the NIST CSF Framework 2.0 Discussion Draft

A24 Limited is a global company that manages critical Payment Hardware Security (HSMs) for Banks and Credit Card Schemes and Payments companies, General Purpose HSMs and Data Protection systems in flight and at rest that rely on and use Cryptography. Due to the nature and security around managing these systems for customers using Cloud Adjacent technologies between legacy systems and Cloud Providers, means that A24 is ensuring high security across private links and networks according to PCI, Critical National Infrastructure and NIST standards for Network Security, Access Controls and Monitoring.

A24 Limited would like to take advantage of the opportunity to provide input into the NIST Cyber Security Framework (CSF) v2.0 discussion draft. Many organisations that A24 Limited work with leverage the NIST CSF. The NIST CSF has become one of the more popular security frameworks, embraced by many industry sectors, and regulatory bodies as the primary method for applying controls and processes to deal with evolving cyber threats.

A24 Limited is proposing addition of metrics (with corresponding notional examples) to the NIST CSF v2 related to four (4) specific functions outlined in the NIST CSF V2 Discussion Draft:

- Govern;
- Identify;
- Protect; &
- Respond

1.1 The Govern Function

Metrics with various associated examples for the Govern function are proposed by A24 Limited for the following Category Identifiers:

- GV.PO
- GV.RM
- GV.RR

1.2 The Identify Function

Metrics with various associated examples for the Identify function are proposed by A24 Limited for the following Category Identifiers:

- ID.SC

1.3 The Protect Function

Metrics with various associated examples for the Protect function are proposed by A24 Limited for the following Category Identifiers:

- PR.AA
- PR.AT
- PR.PS

1.4 The Respond Function

Metrics with various associated examples for the Respond function are proposed by A24 Limited for the following Category Identifiers:

- RS.MA

Appendix: Suggested Metrics Table

Supporting theme #4 "CSF 2.0 will advance understanding of cybersecurity measurement and assessment", A24 Limited believes the NIST CSF 2.0 would be more comprehensive with the inclusion of the suggested additions for metrics and associated notional examples in the following table:

CSF 2.0 Function	CSF 2.0 Category Identifier/Metric	Examples
Govern (GV)	**GV.PO-01** Policies are in place to demonstrate management of end-users.	**Example 01:** Does an Acceptable Use policy exist, and if so, how is it enforced? **Example 01:** What is the policy for employees bringing their own devices (BYOD) to work?
	GV.RM-01 Measurements or methods are in place to demonstrate a level of preparedness for cyber security events to manage risk.	**Example 01:** How many devices on your corporate network have the latest security patches installed? **Example 02:** How many high-risk vulnerabilities have been identified? **Example 03:** How many systems have failed vulnerability scans, and what is the plan to remediate those issues? **Example 04:** How frequently are backups taken, and how are they tested for completeness and accuracy? **Example 05:** How often are disaster recovery, incident response, and business continuity plans tested, and when was the last successful test? **Example 06:** How is your organisation managing data classification and data retention policies, and how are those policies enforced? **Example 07:** What is the frequency of security awareness training for employees, and what metrics are used to measure its effectiveness? **Example 08:** How are security policies and procedures updated and communicated to employees, and how is compliance monitored? **Example 09:** How many devices on your corporate network are running outdated operating systems or software? **Example 10:** How many devices on your network are running end-of-life (EOL) software no longer receiving security updates? **Example 11:** How often are security risk assessments conducted, and what actions are taken because of those assessments? **Example 12:** How are security controls tested for effectiveness and assurance?

		Example 13: How often are security policies and procedures reviewed and updated to reflect changes in the threat landscape? **Example 14:** Do you have processes and plans in place to deal with ransomware? **Example 15:** How do you perform certificate lifecycle management, such as tracking, reporting and managing the status of all issued certificates and their associated entities and to issue notification on pending certificate expiry events? **Example 16:** How are Hardware Security Modules (HSMs) managed, and is there an encryption key management plan in place?
	GV.RR-01 Measurements or methods are in place to provide assurance that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles they are considered for.	**Example 01:** How are background verification checks on all candidates for employment, contractors, and third-party users carried out in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks? **Example 02:** How are definition and enforcement of obligations applied to standard employment and engagement contracts compelling personnel to be aware, adhere and uphold to security policies as they relate to their role?
	GV.RR-02 Measurements or methods are in place for employment termination.	**Example 01:** What processes are in place to provide assurance that employees, contractors, and third-party users no longer have access to systems, applications, or hardware assets once their employment arrangements have been terminated?
Identify (ID)	**ID.SC-01:** Measurements or methods are in place to demonstrate third-party patching effectiveness.	**Example 01:** How frequently are your third-party vendors' systems scanned for vulnerabilities, and how are these scans conducted? **Example 02:** How many risks have been identified in your third-party vendor's systems, and what is the plan to remediate these risks? **Example 03:** How many critical vulnerabilities are yet to be remediated in your vendor's systems? **Example 04:** What is the process for validating vendors have implemented security patches? **Example 05:** What is the process for terminating vendor relationships in the event of poor security performance or failure to comply with security standards? **Example 06:** How is your organization monitoring fourth-party vendor risk (the vendors used by your vendors)? **Example 07:** How is your organization prioritizing patching for third-party vendors based on risk level? **Example 08:** What is the process for communicating patching requirements and deadlines to third-party vendors? **Example 09:** How is your organization tracking compliance with vendor patching requirements and deadlines?
	ID.SC-02: Measurements or methods are in place to determine the time for	**Example 01:** How long does it take for a vendor to respond to security incidents and vulnerabilities?

	third parties to respond to cybersecurity incidents.	**Example 02:** What is the average Mean Time To Respond (MTTR) for your vendor's incident response? **Example 03:** How is incident response coordination managed between your organization and your vendors? **Example 04:** How are security incidents and vulnerabilities communicated to vendors, and how is response progress tracked? **Example 05:** How are vendor response times and incident response performance evaluated and monitored? **Example 06:** How are vendor incident response procedures continually evaluated and improved, and what metrics are used to track this process? **Example 07:** How are incident response procedures for third-party vendors integrated into your overall incident response plan, and how are they updated and communicated to relevant personnel? **Example 08:** How are incident response responsibilities and expectations outlined in service level agreements (SLAs) with third-party vendors, and how are these SLAs monitored and enforced?
	ID.SC-03: Measurements or methods are in place to determine vendor security rating.	**Example 01:** How many vendors are in your organization's supply chain, and what percentage of those vendors are considered high-risk? **Example 02:** What criteria are used to evaluate vendor security, and how are those criteria weighted? **Example 03:** How frequently are vendor security assessments conducted, and what is the process for conducting those assessments? **Example 04:** What types of security ratings or scoring systems are used to evaluate vendor security, and how are those ratings incorporated into the vendor selection process? **Example 05:** How are vendor security ratings monitored and updated over time, and what is the process for reevaluating vendor security when new vulnerabilities or threats emerge? **Example 06:** What is the process for addressing vendor security issues, and how are those issues communicated to the vendor? **Example 07:** How is vendor security performance evaluated and reported to senior management or the board, and what metrics are used to measure vendor security performance?
Protect (PR)	**PR.AA-01** Measurements or methods are in place for access management.	**Example 01:** How is access to sensitive data and systems controlled and monitored, and how is privilege escalation prevented? **Example 02:** What are the different types of user roles and access levels, and how are they defined and documented? **Example 03:** How often are user accounts reviewed and audited for compliance with access policies and procedures? **Example 04:** Are all accounts secured with Muli-Factor Authentication (MFA)? **Example 05:** Have you created password policies addressing

		common malpractices, such as password recycling and weak passwords? **Example 06:** What is the process for monitoring user activity and access logs, and how are suspicious or anomalous behaviours detected and investigated? **Example 07:** What controls are in place to protect privileged accounts? **Example 08:** What are the procedures for granting temporary or emergency access to users, and how are these situations documented and reviewed? **Example 09:** How is access to third-party applications and services managed, and what additional controls are in place to prevent unauthorized access or data leakage? **Example 10:** How are access policies and procedures communicated to users, and what training or awareness programs are in place to promote secure access practices? **Example 11:** How is access granted to new employees, and what is the process for removing access when an employee leaves the company? **Example 12:** What is the process for managing access requests and approvals, and how are these requests documented and tracked? **Example 13:** How is access control regularly audited and reviewed, and how often are access policies and procedures updated? **Example 14:** What are the consequences for non-compliance with access policies, and how is compliance with access policies monitored? **Example 15:** How is access to sensitive data and systems restricted, and how are those restrictions enforced? **Example 16:** How is the principle of least privilege applied to limit user access and reduce the risk of privilege escalation attacks? **Example 17:** What tools and processes are used to monitor user activity and detect potential insider threats?
	PR.AT-01 Measurements or methods are in place for security awareness and training.	**Example 01:** How are employees of the organization and, where relevant, contractors and third-party users made aware of organizational policies and procedures for cyber security, as relevant for their job function? **Example 02:** How is security training provided to ensure employees, contractors and third-party users are trained in cyber security, relevant to their job function.
	PR.PS-01 Measurements or methods are in place to detect intrusion attempts.	**Example 01:** How many intrusion attempts have been detected and blocked by your intrusion detection system? **Example 02:** What is the average time it takes to investigate and respond to detected intrusion attempts? **Example 03:** What is the process for reporting intrusion attempts to relevant stakeholders, including management, legal, and law enforcement? **Example 04:** How many unauthorized access attempts have been detected and blocked by your firewall?

		Example 05: What is the process for investigating and responding to detected intrusion attempts, and how are those findings communicated? **Example 06:** How are logs and other security event data collected and analysed, and what tools and processes are used for this purpose? **Example 07:** How are security incidents classified and prioritized, and what response procedures are in place for each classification? **Example 08:** How frequently are security logs reviewed, and what is the process for reviewing them? **Example 09:** How are security events and incidents correlated and analysed to identify potential threats and attacks? **Example 10:** What measures are in place to prevent false positives and false negatives in intrusion detection systems? **Example 11:** How are network traffic patterns and anomalies monitored to detect potential intrusions? **Example 12:** How are incident response plans updated and tested in response to new intrusion attempts and attack trends? **Example 13:** How are security controls adjusted and fine-tuned based on the results of intrusion detection and response efforts?
	PR.PS-02 Measurements or methods are in place to demonstrate patching effectiveness.	**Example 01:** How frequently are security patches and updates released by software vendors, and how quickly are they implemented? **Example 02:** How are high-risk vulnerabilities prioritized for patching, and what is the process for testing and validating patches before implementation? **Example 03:** How are legacy systems and software that are no longer supported by vendors patched, and what measures are in place to mitigate their security risks? **Example 04:** How are patches and updates distributed and installed across different devices and systems, and how is this process managed and monitored? **Example 05:** What is the average time it takes to apply patches once they are released, and what is the maximum acceptable patching window for high-risk vulnerabilities? **Example 06:** What metrics are used to track patching effectiveness and compliance, and how are these metrics used to drive improvements in the patching process? **Example 07:** How are patches validated to ensure they do not cause any conflicts or disruptions in the systems they are being applied to? **Example 08:** How are legacy systems and applications that are no longer supported with security patches being handled? Is there a plan in place for dealing with these systems? **Example 09:** Are there any exceptions to the patching process, such as certain systems or applications that cannot be patched for operational or other reasons? How are these exceptions managed and mitigated?

	PR.PS-03 Measurements or methods are in place to detect unidentified devices on internal networks.	**Example 01:** What is the inventory of authorized devices on your network, and how is it maintained and kept up to date? **Example 02:** How many assets are there in your network? **Example 03:** How many of those assets store sensitive data? **Example 04:** What is the process for responding to unauthorized devices on the network, and how are these devices quarantined and monitored? **Example 05:** How are IoT devices secured, and what is the process for monitoring and patching their vulnerabilities? **Example 06:** How is network segmentation implemented, and how are different types of devices segregated on the network? **Example 07:** How are access controls implemented for devices on your network, and what is the process for granting and revoking access permissions? **Example 08:** How are devices authenticated and authorized before being allowed to connect to the network? **Example 09:** What is the policy for employees bringing their own devices (BYOD) to work, and how are these devices managed and secured? **Example 10:** What measures are in place to detect and respond to rogue access points or other unauthorized network infrastructure? **Example 11:** What is the process for tracking the lifecycle of devices on your network, including acquisition, deployment, maintenance, and retirement? **Example 12:** How are third-party devices and services securely integrated into your network, and what is the process for managing their access and permissions? **Example 13:** What is the policy for remote access to your network, and what measures are in place to secure and monitor remote connections?
Respond (RS)	**RS.MA-01** Measurements or methods are in place to handle security incidents.	**Example 01:** How many security incidents have been detected and resolved in the past month/quarter/year? **Example 02:** How many successful cyber-attacks have occurred in the past month/quarter/year? **Example 03:** What types of incidents have occurred, and what was the impact of each incident? **Example 04:** What metrics are used to track incident response and resolution times, and how are these metrics used to improve the incident response process? **Example 05:** How is data recovery managed in the event of a security incident, and how are backups tested and validated? **Example 06:** What is the root cause analysis of each incident, and what corrective actions were taken to prevent similar incidents from occurring in the future? **Example 07:** What is the average downtime experienced during a security incident, and what is the impact on the organization's operations? **Example 08:** What is the average cost associated with a

		security incident, including costs for incident response, remediation, and reputational damage? **Example 09:** How is user behaviour monitored to identify potential security incidents or insider threats? **Example 10:** How is threat intelligence gathered and used to proactively detect and prevent security incidents? **Example 11:** What is the process for reporting security incidents to regulatory authorities, customers, and other stakeholders? **Example 12:** How is the organization's incident response plan updated and tested to ensure it remains effective and relevant?

End of Document