**NIST IR 8477-Based Set Theory Relationship Mapping (STRM)**
**Reference Document:** Secure Controls Framework (SCF) version 2026.2
**STRM Guidance:** https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

**Focal Document:** Singapore - Cyber Hygiene Practice (2019)
**Focal Document URL:** https://www.mas.gov.sg/-/media/MAS/Notices/PDF/MAS-Notice-132.pdf
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-cyber-hygiene-practice-2019.pdf

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|---|---|---|---|---|---|---|---|---|---|
| I | Introduction | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| II | Definitions | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| III | Application of Notice | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| IV | Cyber Hygiene Practices | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 4.1 | Administrative Accounts | A relevant entity must ensure that every administrative account in respect of any operating system, database, application, security appliance or network device, is secured to prevent any unauthorised access to or use of such account. | Functional | Subset Of | Identity & Access Management (IAM) | IAC-01 | Mechanisms exist to facilitate the implementation of identification and access management controls. | 10 | |
| 4.1 | Administrative Accounts | A relevant entity must ensure that every administrative account in respect of any operating system, database, application, security appliance or network device, is secured to prevent any unauthorised access to or use of such account. | Functional | Intersects With | Account Management | IAC-15 | Mechanisms exist to:<br>(1) Define authorized system account types;<br>(2) Define prohibited system account types; and<br>(3) Proactively govern individual, group, system, service, application, guest and temporary accounts. | 8 | |
| 4.1 | Administrative Accounts | A relevant entity must ensure that every administrative account in respect of any operating system, database, application, security appliance or network device, is secured to prevent any unauthorised access to or use of such account. | Functional | Intersects With | Privileged Account Management (PAM) | IAC-16 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 8 | |
| 4.2 | Security Patches | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 4.2(a) | Security Patches | A relevant entity must ensure that security patches are applied to address vulnerabilities to every system, and apply such security patches within a timeframe that is commensurate with the risks posed by each vulnerability. | Functional | Intersects With | Vulnerability Remediation Process | VPM-02 | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. | 5 | |
| 4.2(a) | Security Patches | A relevant entity must ensure that security patches are applied to address vulnerabilities to every system, and apply such security patches within a timeframe that is commensurate with the risks posed by each vulnerability. | Functional | Intersects With | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 5 | |
| 4.2(b) | Security Patches | Where no security patch is available to address a vulnerability, the relevant entity must ensure that controls are instituted to reduce any risk posed by such vulnerability to such a system. | Functional | Subset Of | Compensating Countermeasures | RSK-06.2 | Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats. | 10 | |
| 4.3 | Security Standards | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| 4.3(a) | Security Standards | A relevant entity must ensure that there is a written set of security standards for every system. | Functional | Intersects With | Publishing Security, Compliance & Resilience Documentation | GOV-02 | Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities. | 5 | |
| 4.3(a) | Security Standards | A relevant entity must ensure that there is a written set of security standards for every system. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | |
| 4.3(a) | Security Standards | A relevant entity must ensure that there is a written set of security standards for every system. | Functional | Intersects With | Applied Security, Compliance and Resilience Controls Documentation | IAO-03 | Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:<br>(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);<br>(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and<br>(3) Provides a historical record of applied security controls, including changes. | 5 | |
| 4.3(b) | Security Standards | Subject to sub-paragraph (c), a relevant entity must ensure that every system conforms to the set of security standards. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | |
| 4.3(b) | Security Standards | Subject to sub-paragraph (c), a relevant entity must ensure that every system conforms to the set of security standards. | Functional | Intersects With | Configuration Enforcement | CFG-06 | Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices. | 5 | |
| 4.3(c) | Security Standards | Where the system is unable to conform to the set of security standards, the relevant entity must ensure that controls are instituted to reduce any risk posed by such non-conformity. | Functional | Intersects With | Compensating Countermeasures | RSK-06.2 | Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats. | 5 | |
| 4.4 | Network Perimeter Defense | A relevant entity must implement controls at its network perimeter to restrict all unauthorised network traffic. | Functional | Subset Of | Network Security Controls (NSC) | NET-01 | Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC). | 10 | |
| 4.4 | Network Perimeter Defense | A relevant entity must implement controls at its network perimeter to restrict all unauthorised network traffic. | Functional | Intersects With | Boundary Protection | NET-03 | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network. | 5 | |
| 4.4 | Network Perimeter Defense | A relevant entity must implement controls at its network perimeter to restrict all unauthorised network traffic. | Functional | Intersects With | Deny Traffic by Default & Allow Traffic by Exception | NET-04.1 | Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception). | 5 | |
| 4.5 | Malware protection | A relevant entity must ensure that one or more malware protection measures are implemented on every system, to mitigate the risk of malware infection, where such malware protection measures are available and can be implemented. | Functional | Intersects With | Malicious Code Protection (Anti-Malware) | END-04 | Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code. | 5 | |
| 4.6 | Multi-factor Authentication | Subject to paragraph 4.7, a relevant entity must ensure that multi-factor authentication is implemented for the following: | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:<br>(1) Remote network access;<br>(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or<br>(3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data. | 5 | |
| 4.6(a) | Multi-factor Authentication | all administrative accounts in respect of any operating system, database, application, security appliance or network device that is a critical system; and | Functional | Intersects With | Network Access to Privileged Accounts | IAC-06.1 | Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts. | 5 | |
| 4.6(b) | Multi-factor Authentication | all accounts on any system used by the relevant entity to access customer information through the internet. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:<br>(1) Remote network access;<br>(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or<br>(3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data. | 5 | |
| 4.6(b) | Multi-factor Authentication | all accounts on any system used by the relevant entity to access customer information through the internet. | Functional | Intersects With | Network Access to Non-Privileged Accounts | IAC-06.2 | Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts. | 5 | |
| 4.7 | N/A | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | |
| V | Effective Date | See FDE for details. | Functional | No Relationship | N/A | N/A | N/A | 0 | |