NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document : Secure Controls Framework (SCF) version 2025.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: Australia Essential 8
Focal Document URL: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-apac-australia-essential-8.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 (optional)	Notes (optional)
Principle 1	N/A	Patch applications	Functional	intersects with	Vulnerability Exploitation Analysis	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	5	
Principle 1	N/A	Patch applications	Functional	intersects with	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: (1) Replacing systems when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported system components required to satisfy mission/business needs.	5	
Principle 1	N/A	Patch applications	Functional	intersects with	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	
Principle 1	N/A	Patch applications	Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
Principle 1	N/A	Patch applications	Functional	intersects with	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	5	
Principle 1	N/A	Patch applications	Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
Principle 1	N/A	Patch applications	Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
Principle 1	N/A	Patch applications	Functional	intersects with	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5	
Principle 1	N/A	Patch applications	Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
Principle 1	N/A	Patch applications	Functional	intersects with	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
Principle 1	N/A	Patch applications	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
Principle 2	N/A	Patch operating systems	Functional	intersects with	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	
Principle 2	N/A	Patch operating systems	Functional	intersects with	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5	
Principle 2	N/A	Patch operating systems	Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
Principle 2	N/A	Patch operating systems	Functional	intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
Principle 2	N/A	Patch operating systems	Functional	intersects with	Vulnerability Exploitation Analysis	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	5	
Principle 2	N/A	Patch operating systems	Functional	intersects with	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
Principle 2	N/A	Patch operating systems	Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
Principle 2	N/A	Patch operating systems	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
Principle 2	N/A	Patch operating systems	Functional	intersects with	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: (1) Replacing systems when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported system components required to satisfy mission/business needs.	5	
Principle 2	N/A	Patch operating systems	Functional	intersects with	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	5	
Principle 2	N/A	Patch operating systems	Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
Principle 3	N/A	Multi-factor authentication	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	
Principle 3	N/A	Multi-factor authentication	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	
Principle 3	N/A	Multi-factor authentication	Functional	intersects with	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
Principle 3	N/A	Multi-factor authentication	Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
Principle 4	N/A	Restrict administrative privileges	Functional	intersects with	Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to organization-defined personnel or roles without management approval.	5	
Principle 4	N/A	Restrict administrative privileges	Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
Principle 4	N/A	Restrict administrative privileges	Functional	intersects with	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
Principle 4	N/A	Restrict administrative privileges	Functional	intersects with	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
Principle 4	N/A	Restrict administrative privileges	Functional	intersects with	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.	5	
Principle 4	N/A	Restrict administrative privileges	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	
Principle 4	N/A	Restrict administrative privileges	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
Principle 5	N/A	Application control	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
Principle 5	N/A	Application control	Functional	intersects with	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
Principle 5	N/A	Application control	Functional	subset of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	
Principle 5	N/A	Application control	Functional	intersects with	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
Principle 5	N/A	Application control	Functional	intersects with	Restrict Roles Permitted To Install Software	CFG-05.2	Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.	5	
Principle 5	N/A	Application control	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
Principle 5	N/A	Application control	Functional	subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
Principle 5	N/A	Application control	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
Principle 6	N/A	Restrict Microsoft Office macros	Functional	intersects with	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
Principle 6	N/A	Restrict Microsoft Office macros	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
Principle 6	N/A	Restrict Microsoft Office macros	Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
Principle 6	N/A	Restrict Microsoft Office macros	Functional	subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
Principle 6	N/A	Restrict Microsoft Office macros	Functional	intersects with	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
Principle 6	N/A	Restrict Microsoft Office macros	Functional	intersects with	Restrict Roles Permitted To Install Software	CFG-05.2	Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.	5	
Principle 7	N/A	User application hardening	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
Principle 7	N/A	User application hardening	Functional	intersects with	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
Principle 7	N/A	User application hardening	Functional	subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
Principle 7	N/A	User application hardening	Functional	subset of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	
Principle 7	N/A	User application hardening	Functional	intersects with	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
Principle 8	N/A	Regular backups	Functional	intersects with	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Principle 8	N/A	Regular backups	Functional	intersects with	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
Principle 8	N/A	Regular backups	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	