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: UK - Cyber Essentials: Requirements for IT Infrastructure v3.3
Focal Document URL: https://www.ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-3.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-gbr-cyber-essentials-requirements-3-3.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
1	Firewalls	You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality).	Functional	Intersects With	Software Firewall	END-05	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all endpoint devices, where technically feasible.	8	To make sure that only secure and necessary network services can be accessed from the internet.
1	Firewalls	You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality).	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	To make sure that only secure and necessary network services can be accessed from the internet.
2	Secure Configuration	Your organisation must proactively manage your computers and network devices. You must regularly:	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	Ensure that computers and network devices are properly configured to: • reduce vulnerabilities • provide only the services required to fulfil their role
2-BP1	Secure Configuration	remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5	
2-BP1	Secure Configuration	remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
2-BP1	Secure Configuration	remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)	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	
2-BP2	Secure Configuration	change any default or guessable account passwords (see password-based authentication)	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
2-BP3	Secure Configuration	remove or disable unnecessary software (including applications, system utilities and network services)	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	
2-BP3	Secure Configuration	remove or disable unnecessary software (including applications, system utilities and network services)	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
2-BP4	Secure Configuration	disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded)	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	
2-BP5	Secure Configuration	ensure users are authenticated before allowing them access to organisational data or services	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
2-BP6	Secure Configuration	ensure appropriate device locking controls (see 'device unlocking', below) for users that are physically present	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
3	Security Update Management	You must make sure that all software in scope is kept up to date. All software on in-scope devices must:	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.	8	Ensure that devices and software are not vulnerable to known security issues for which fixes are available.
3-BP1	Security Update Management	be licensed and supported	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5	
3-BP2	Security Update Management	be removed from devices when it becomes unsupported, or removed from scope by using a defined sub-set that prevents all traffic to or from the	Functional	Intersects With	Unsupported Technology Assets, Applications	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by:	8	
3-BP3	Security Update Management	have automatic updates enabled where possible	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	8	
3-BP4	Security Update Management	be updated, including vulnerability fixes, within 14 days* of release, where:	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	5	
3-BP4-1	Security Update Management	the update fixes vulnerabilities described by the vendor as 'critical' or 'high risk'	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	
3-BP4-2	Security Update Management	the update addresses vulnerabilities with a CVSS v3 base score of 7 or above	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	
3-BP4-3	Security Update Management	there are no details of the level of vulnerabilities that the update fixes provided by the vendor	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	User Access Control	Your organisation must be in control of your user accounts and the access privileges that allow access to your organisational data and services. It's important to note that this also includes third party accounts – for	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Ensure that user accounts: • are assigned to authorised individuals only
4	User Access Control	Your organisation must be in control of your user accounts and the access privileges that allow access to your organisational data and services. It's important to note that this also includes third party accounts – for example, accounts used by your support services. You also need to understand how user accounts authenticate and manage the authentication accordingly. This means your organisation must:	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	Ensure that user accounts: • are assigned to authorised individuals only • provide access to only those applications, computers and networks that the user needs to carry out their role
4-BP1	User Access Control	have in place a process to create and approve user accounts	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5	
4-BP2	User Access Control	authenticate users with unique credentials before granting access to applications or devices	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
4-BP3	User Access Control	remove or disable user accounts when they're no longer required (for example, when a user leaves the organisation or after a defined period of account inactivity)	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5	
4-BP3	User Access Control	remove or disable user accounts when they're no longer required (for example, when a user leaves the organisation or after a defined period of account inactivity)	Functional	Intersects With	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5	
4-BP4	User Access Control	implement MFA, where available – authentication to cloud services must always use MFA	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 Technology Assets, Applications and/or Services (TAAS); and/ or	5	
4-BP5	User Access Control	use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)	Functional	Intersects With	Dedicated Privileged Account	IAC-16.4	Mechanisms exist to assign dedicated privileged user accounts to be used solely for duties requiring privileged access.	5	
4-BP6	User Access Control	remove or disable special access privileges when no longer required (when a member of staff changes role, for example)	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
4-BP6	User Access Control	remove or disable special access privileges when no longer required (when a member of staff changes role, for example)	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).	5	
5	Malware protection	You must make sure that a malware protection mechanism is active on all devices in scope. For each device, you must use at least one of the	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	To restrict execution of known malware and untrusted software, from causing

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: UK - Cyber Essentials: Requirements for IT Infrastructure v3.3

Focal Document URL: https://www.ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-3.pdf

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-gbr-cyber-essentials-requirements-3-3.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
5-BP1	Anti-malware software	If you use anti-malware software to protect your device it must be configured to:	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
5-BP1-1	Anti-malware software	be updated in line with vendor recommendations	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
5-BP1-2	Anti-malware software	prevent malware from running	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management	5	
5-BP1-3	Anti-malware software	prevent the execution of malicious code	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by	5	
5-BP1-4	Anti-malware software	prevent connections to malicious websites over the internet	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
5-BP2	Application allow listing	Only approved applications, restricted by code signing, are allowed to execute on devices. You must:	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
5-BP2-1	Application allow listing	actively approve such applications before deploying them to devices	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
5-BP2-2	Application allow listing	maintain a current list of approved applications, users must not be able to install any application that is unsigned or has an invalid signature	Functional	Intersects With	Approved Technologies	AST-01.4	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
5-BP2-2	Application allow listing	maintain a current list of approved applications, users must not be able to install any application that is unsigned or has an invalid signature	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	