NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Cyber Resilience Capability Maturity Model (CR-CMM) (2026)
https://cr-cmm.org/
https://securecontrolsframework.com/content/strm/scf-strm-general-cr-cmm-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CR1.1.5	N/A	A dedicated process is in place to assess the asset criticality of technology applications or platforms (IT BIA).	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
CR1.1.4	N/A	Upstream and downstream dependencies (people, process, technology, third-party) have been documented for the critical services.	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
CR1.1.1	N/A	An approved Business Impact Analysis (BIA) has identified which business services are critical.	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5	
CR1.1.4	N/A	Upstream and downstream dependencies (people, process, technology, third-party) have been documented for the critical services.	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
CR2.2.1	N/A	Logs from critical systems (e.g. EDR, Active Directory, firewalls) are centralized into a monitored analytics platform (e.g. SIEM).	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
CR2.2.4	N/A	Threat hunting hypotheses and results are integrated into monthly detection-rule performance reviews.	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	5	
CR2.2.6	N/A	Indicators of Behavior IoB are preferred over Indicators of Compromise IoC in the detection design phase.	THR-11	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	5	
CR3.3.2	N/A	Breach and attack simulation or continuous exposure management tools continuously test telemetry and controls.	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
CR3.1.2	N/A	Threat models are built considering critical assets and fed as scenario input to the SOC and architecture teams.	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
CR3.1.1	N/A	Priority threat actors are defined based on industry exposure and associated with MITRE ATT&CK techniques.	MON-16.2	Mechanisms exist to monitor third-party personnel activity for potential security incidents.	5	
CR3.1.6	N/A	Voice-of-Adversary or PETE analysis is used by offensive security specialists to stress-test architectural designs.	PRM-02.1	Mechanisms exist to integrate foundational cybersecurity practices with advanced technologies to maintain situation awareness of and minimize the organization's exposure to evolving risks and threats.	5	
CR4.3.6	N/A	Advanced design patterns such as modularity, moving-target defense, and deceptive architectures continuously evolve based on predictive CTI.	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
CR4.1.5	N/A	Progress toward the zero trust roadmap is tracked and reported to leadership.	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	5	
CR4.1.3	N/A	Deception mechanisms (e.g., honeypots) are deployed in critical segments.	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for Technology Assets, Applications and/or Services (TAAS) to confuse and mislead adversaries.	5	
CR4.1.7	N/A	Micro segmentation policies adapt dynamically to risk context.	IRO-02.3	Automated mechanisms exist to dynamically reconfigure system components as part of the incident response capability.	5	
CR4.3.1	N/A	Cyber resilience principles (e.g. interoperability, redundancy, immutability, heterogeneity) are considered in every new or existing design.	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
CR4.3.1	N/A	Cyber resilience principles (e.g. interoperability, redundancy, immutability, heterogeneity) are considered in every new or existing design.	SEA-01.3	Mechanisms exist to ensure security, compliance and resilience are designed and implemented to provide resistance to: (1) Unintentional errors (by users or software); and (2) Intentional attack or circumvention.	5	
CR5.1.9	N/A	Fall back operations are defined to ensure the organization can remain viable (e.g., operate above minimum viable levels) until full operational capability is restored.	BCD-07	Mechanisms exist to implement alternative or compensating controls to satisfy security functions when the primary means of implementing the security function is unavailable or compromised.	5	
CR5.1.1	N/A	A cyber crisis policy is formally approved by the Board, including pre-approved decisions (e.g. highest financial impact thresholds).	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
CR5.2.1	N/A	Internal and external communication templates are pre-approved by Legal and PR corporate communications.	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
CR5.1.2	N/A	Crisis roles, decision rights, and escalation paths are documented and communicated.	BCD-01.7	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5	
CR5.2.6	N/A	Critical services are equipped with additional out-of-band communication channels, including analog methods (e.g. regular phone lines) in case of digital compromise.	BCD-10.4	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable.	5	
CR5.3.2	N/A	Contact information, including from non-connected corporate devices of external partners, is maintained and available to the response team.	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
CR5.3.2	N/A	Contact information, including from non-connected corporate devices of external partners, is maintained and available to the response team.	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	5	
CR6.2.2	N/A	Simulations are aligned to critical asset attack paths and current threat actors.	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5	
CR6.2.6	N/A	Covert red-blue, including black- and white-box scenarios, are executed to validate extreme-but-plausible threats.	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	5	
CR6.3.2	N/A	Simulations engage all relevant functions (legal, HR, supply-chain, finance) at different levels of seniority.	IRO-05.1	Mechanisms exist to incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.	5	
CR6.2.2	N/A	Simulations are aligned to critical asset attack paths and current threat actors.	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5	
CR6.3.1	N/A	The organization has a formal policy governing scenario-based testing within its business continuity program.	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	5	
CR7.2.1	N/A	Fail-over procedures are documented and, where feasible, automated and orchestrated.	BCD-03.2	Automated mechanisms exist to provide a more thorough and realistic contingency training environment.	5	
CR7.2.2	N/A	Drills are executed to validate RTO assumptions for each critical service.	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	10	
CR7.2.8	N/A	Fail over and resumption drills include a review and validation of IR, DR, and BCP playbooks to ensure that containment, eradication, and recovery steps are coordinated for destructive cyber scenarios.	BCD-04.1	Mechanisms exist to coordinate contingency plan testing with internal and external elements responsible for related plans.	5	
CR7.3.6	N/A	Continuity and DR tests with critical third parties explicitly validate integration between the provider's DR / BCP plans and the organization's crisis management, business continuity, and cyber recovery procedures.	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
CR7.2.13	N/A	Lessons learned from fail over and resumption drills (including forensic readiness and segmentation gaps) are systematically captured, risk rated, and fed into an improvement or hardening roadmap for contingency capabilities.	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services) (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing activities.	5	
CR8.1.2	N/A	Security testing is embedded in CI/CD pipelines for critical applications.	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5	
CR8.3.1	N/A	Load and stress tests are run for critical services ahead of major releases.	TDA-02.10	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for an appropriate level of security and resiliency based on applicable risks and threats.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CR8.2.1	N/A	Vulnerability scans are immediately run after patch deployment on critical systems.	VPM-05.6	Mechanisms exist to perform due diligence on software and/or firmware update stability by conducting pre-production testing in a non-production environment.	5	
CR9.1.1	N/A	Penetration-testing scope is threat-informed, risk-based and inclusive of IT, OT, Cloud, and AI environments.	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	
CR9.3.2	N/A	Physical red teaming is implemented.	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	5	
CR6.2.6	N/A	Covert red-blue, including black- and white-box scenarios, are executed to validate extreme-but-plausible threats.	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
CR10.1.1	N/A	Recovery plans exist for every critical service and asset.	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	5	
CR10.4.4	N/A	Backup validation is effective in ensuring integrity after potential attacker dwell time.	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	
CR10.4.4	N/A	Backup validation is effective in ensuring integrity after potential attacker dwell time.	BCD-13.1	Mechanisms exist to verify the integrity of backups and other restoration assets prior to using them for restoration.	5	
CR10.2.4	N/A	A data-vault or secure offline copy environment is in place for critical datasets.	BCD-11.8	Mechanisms exist to implement and enforce dual authorization for the deletion or destruction of sensitive backup media and data.	5	
CR10.2.6	N/A	Recovery drills are executed from the isolated vault to a clean environment.	BCD-11.3	Mechanisms exist to reimage assets from configuration-controlled and integrity-protected images that represent a secure, operational state.	5	
CR10.2.6	N/A	Recovery drills are executed from the isolated vault to a clean environment.	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
CR10.2.4	N/A	A data-vault or secure offline copy environment is in place for critical datasets.	BCD-14	Mechanisms exist to utilize an isolated, non-production environment to perform data backup and recovery operations through offline, cloud or off-site capabilities.	5	
CR10.2.5	N/A	Business continuity plans (BCP) are integrated with the isolated recovery environment and resumption processes.	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5	