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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - NSF Research Infrastructure Guide (January 2025) - Sections 5.2-5.3 (Cyberinfrastructure & Information Assurance)
Focal Document URL: https://www.nsf.gov/bfa/lfo/lfo_documents.jsp
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-nsf-rig-2025-information-assurance.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	Legecy SCF #
5.2	Cyberinfrastructure	Cyberinfrastructure (CI) is the ensemble of computational, data, control, and user-focused software and middleware, networking, and cybersecurity infrastructure and associated policies, standards, protocols, and staffing needed to accomplish the scientific mission for Major Facility or Mid-scale RI. Effective planning and oversight ensure cybersecurity, scalability, and alignment with scientific missions. Major Facilities and Mid-scale RI must develop a Cyberinfrastructure Plan.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	3		GOV-01
5.3	Information Assurance	Rigorous measures protect against cyber threats and unauthorized access, ensuring the confidentiality, availability, and reliability of research data through a comprehensive program.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	8		GOV-01
5.3	Information Assurance	Rigorous measures protect against cyber threats and unauthorized access, ensuring the confidentiality, availability, and reliability of research data through a comprehensive program.	Functional	Intersects With	Information Assurance (IA) Operations	IAO-02	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8		IAO-01
5.3.1	Introduction	IA is fundamentally a program of risk management and is the responsibility of the management organizations of Awardees. NSF Major Facilities and Mid-scale RI Project Teams must develop and implement an IA Program and associated IA Management Plan (IAMP), appropriately scaled and tailored to the size, complexity and technical nature of the funded activities. The IA Program is a set of measures taken together to protect and defend information and information systems; the IAMP is the high-level narrative summary of the IA Program. NSF expects facilities to strive for resilience: minimizing the likelihood of successful attacks, minimizing the impact of sophisticated attacks, minimizing the period of disruption of scientific operations, and ensuring the integrity of scientific data and artifacts despite the occurrence of a cybersecurity incident.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	8		GOV-01
5.3.1	Introduction	IA is fundamentally a program of risk management and is the responsibility of the management organizations of Awardees. NSF Major Facilities and Mid-scale RI Project Teams must develop and implement an IA Program and associated IA Management Plan (IAMP), appropriately scaled and tailored to the size, complexity and technical nature of the funded activities. The IA Program is a set of measures taken together to protect and defend information and information systems; the IAMP is the high-level narrative summary of the IA Program. NSF expects facilities to strive for resilience: minimizing the likelihood of successful attacks, minimizing the impact of sophisticated attacks, minimizing the period of disruption of scientific operations, and ensuring the integrity of scientific data and artifacts despite the occurrence of a cybersecurity incident.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (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 (3) Provides a historical record of applied security controls, including changes.	5		IAO-03
5.3.2	Framing IA Risks in the Contemporary Threat Landscape	RI faces a wide array of threats and pressures that require attention. NSF expects RI to include cyber risks in the Risk Register. Four areas are detailed to assist with establishing the cyber risk elements of a Risk Register and to provide situational awareness.	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	5		RSK-03
5.3.2	Framing IA Risks in the Contemporary Threat Landscape	RI faces a wide array of threats and pressures that require attention. NSF expects RI to include cyber risks in the Risk Register. Four areas are detailed to assist with establishing the cyber risk elements of a Risk Register and to provide situational awareness.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5		THR-01
5.3.2.1	N/A	Geopolitics: The state of the U.S. relationship with several adversarial countries directly impacts cybersecurity operations. Countries on the OFAC sanctioned list or with ITAR restrictions warrant special note. CISA and the FBI are effective partners in staying abreast of national security threats.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	3		THR-01
5.3.2.2	N/A	Specific Research Domains: Facilities that work in specific domains or with nationally critical or emerging technology should recognize that this work may attract the attention of state actors. These domains include export-controlled data, research involving technology on the Critical and Emerging Technologies List, vaccine development, or defense related research.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	3		THR-01
5.3.2.3	N/A	Regulatory Pressures: Regulations that address cybersecurity practices continue to be advanced by the federal government and many federal agencies (e.g., NSPM-33 and OSTP memos identify cybersecurity as a core component of research security programs; CUI requirements; privacy regulations). Facilities should monitor the activities of all agencies they interact with and examine these for potential impact on NSF sponsored programs.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
5.3.2.4	N/A	Other Attacks and Concerns: Security professionals are faced with a variety of exigent and emerging attack types (e.g., ransomware, supply chain management, MFA fatigue). Items such as these should be evaluated at least bi-annually, and mitigation plans developed or updated.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	3		THR-01
5.3.3	Awardee Obligations	There are several requirements relevant to IA for Awardees: Uniform Guidance 200.303 (internal controls including technology infrastructure and security management); the Cooperative Agreement Supplemental Financial and Administrative Terms and Conditions require an information security program with required components described in the IAMP; a tailored, scaled, and progressively elaborated IAMP is a required element of the Design, Construction/Implementation, and Operations Stages; where funded through a contract, FAR 4.1903 and FAR 52.204-21 requirements for Safeguarding of Covered Information Systems apply. NSF expects to be provided at all program reviews: the IAMP, a current IA budget, a list of cyber related risks and intended mitigations as part of the Risk Register, and an update on the status of the critical technical controls.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5		CPL-01
5.3.3	Awardee Obligations	There are several requirements relevant to IA for Awardees: Uniform Guidance 200.303 (internal controls including technology infrastructure and security management); the Cooperative Agreement Supplemental Financial and Administrative Terms and Conditions require an information security program with required components described in the IAMP; a tailored, scaled, and progressively elaborated IAMP is a required element of the Design, Construction/Implementation, and Operations Stages; where funded through a contract, FAR 4.1903 and FAR 52.204-21 requirements for Safeguarding of Covered Information Systems apply. NSF expects to be provided at all program reviews: the IAMP, a current IA budget, a list of cyber related risks and intended mitigations as part of the Risk Register, and an update on the status of the critical technical controls.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
5.3.3	Awardee Obligations	There are several requirements relevant to IA for Awardees: Uniform Guidance 200.303 (internal controls including technology infrastructure and security management); the Cooperative Agreement Supplemental Financial and Administrative Terms and Conditions require an information security program with required components described in the IAMP; a tailored, scaled, and progressively elaborated IAMP is a required element of the Design, Construction/Implementation, and Operations Stages; where funded through a contract, FAR 4.1903 and FAR 52.204-21 requirements for Safeguarding of Covered Information Systems apply. NSF expects to be provided at all program reviews: the IAMP, a current IA budget, a list of cyber related risks and intended mitigations as part of the Risk Register, and an update on the status of the critical technical controls.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	5		GOV-01

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - NSF Research Infrastructure Guide (January 2025) - Sections 5.2-5.3 (Cyberinfrastructure & Information Assurance)
Focal Document URL: https://www.nsf.gov/bfa/lfo/lfo_documents.jsp
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-nsf-rig-2025-information-assurance.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	Legacy SCF #
5.3.3.1	N/A	IA Program Tailoring and Scaling: An IA Program should naturally reflect the nature and scope of a facility, and materials describing the program should be tailored and scaled. Mid-scale RI may rely on institutional information security programs; Major Facilities typically build stand-alone security programs that are considerably more comprehensive and rigorous. Over time, the IAMP should be progressively elaborated to reflect the increasing maturity of the IA Program.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	3		GOV-01
5.3.4	Cyber Risk in the Risk Register	Cyber risk should be included as a category in the Risk Register and systematically addressed through a Risk Management Plan. Cyber risks should be categorized as such in the Risk Register; a review of cyber risks in the Risk Register should take place at least quarterly. Sub-categories may include strategic risks, exigent or emerging risks, and operational risks. A reasonably complete set of risks requires input from facility management, scientists and researchers, and CI and cybersecurity professionals.	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	5		RSK-03
5.3.4	Cyber Risk in the Risk Register	Cyber risk should be included as a category in the Risk Register and systematically addressed through a Risk Management Plan. Cyber risks should be categorized as such in the Risk Register; a review of cyber risks in the Risk Register should take place at least quarterly. Sub-categories may include strategic risks, exigent or emerging risks, and operational risks. A reasonably complete set of risks requires input from facility management, scientists and researchers, and CI and cybersecurity professionals.	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	8		RSK-04.1
5.3.5	Information Assurance Management Plan	Created by the IA Lead, the IAMP is the high-level management runbook for an IA Program, codifying the program's scope, roles and responsibilities, governance, and controls. Required elements: Statement of Cyber Risk Management Strategy (including a cybersecurity framework and baseline cybersecurity control set); Scope and Boundaries; Responsibility Model and Matrix; Governance; Risk Treatment Plans; IA Program Operations (programmatic processes, baseline security functions such as incident response, email anti-spam and malware protections, account management, MFA, vulnerability detection and patching, and supplemental responsibilities); and an Assessment Plan.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	3		GOV-04
5.3.5	Information Assurance Management Plan	Created by the IA Lead, the IAMP is the high-level management runbook for an IA Program, codifying the program's scope, roles and responsibilities, governance, and controls. Required elements: Statement of Cyber Risk Management Strategy (including a cybersecurity framework and baseline cybersecurity control set); Scope and Boundaries; Responsibility Model and Matrix; Governance; Risk Treatment Plans; IA Program Operations (programmatic processes, baseline security functions such as incident response, email anti-spam and malware protections, account management, MFA, vulnerability detection and patching, and supplemental responsibilities); and an Assessment Plan.	Functional	Intersects With	Information Assurance (IA) Operations	IAO-02	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	8		IAO-01
5.3.5	Information Assurance Management Plan	Created by the IA Lead, the IAMP is the high-level management runbook for an IA Program, codifying the program's scope, roles and responsibilities, governance, and controls. Required elements: Statement of Cyber Risk Management Strategy (including a cybersecurity framework and baseline cybersecurity control set); Scope and Boundaries; Responsibility Model and Matrix; Governance; Risk Treatment Plans; IA Program Operations (programmatic processes, baseline security functions such as incident response, email anti-spam and malware protections, account management, MFA, vulnerability detection and patching, and supplemental responsibilities); and an Assessment Plan.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (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 (3) Provides a historical record of applied security controls, including changes.	8		IAO-03
5.3.5	Information Assurance Management Plan	Created by the IA Lead, the IAMP is the high-level management runbook for an IA Program, codifying the program's scope, roles and responsibilities, governance, and controls. Required elements: Statement of Cyber Risk Management Strategy (including a cybersecurity framework and baseline cybersecurity control set); Scope and Boundaries; Responsibility Model and Matrix; Governance; Risk Treatment Plans; IA Program Operations (programmatic processes, baseline security functions such as incident response, email anti-spam and malware protections, account management, MFA, vulnerability detection and patching, and supplemental responsibilities); and an Assessment Plan.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5		RSK-01
5.3.6	Critical Controls	Several cybersecurity controls have been identified as exceptionally impactful in improving the resilience of Major Facility and Mid-scale RI. NSF expects these controls to be an integral part of the Awardee's management practices and to be targeted for prioritized implementation, integrated into the design and construction of new RI, and phased into operational RI within a reasonable timeframe. Compensating controls or novel approaches to addressing a control are welcomed.	Functional	Intersects With	Select Controls	GOV-11.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15.1
5.3.6	Critical Controls	Several cybersecurity controls have been identified as exceptionally impactful in improving the resilience of Major Facility and Mid-scale RI. NSF expects these controls to be an integral part of the Awardee's management practices and to be targeted for prioritized implementation, integrated into the design and construction of new RI, and phased into operational RI within a reasonable timeframe. Compensating controls or novel approaches to addressing a control are welcomed.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	3		RSK-06.2
5.3.6 / NSF1	N/A	Require phishing resistant MFA for all privileged/administrator accounts (accounts with system management privileges or the ability to change a system or an application's configuration). REF: IA-2(1), AC-2(7) 800-53r5.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5		IAC-16
5.3.6 / NSF1	N/A	Require phishing resistant MFA for all privileged/administrator accounts (accounts with system management privileges or the ability to change a system or an application's configuration). REF: IA-2(1), AC-2(7) 800-53r5.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	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 (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	8		IAC-06
5.3.6 / NSF1	N/A	Require phishing resistant MFA for all privileged/administrator accounts (accounts with system management privileges or the ability to change a system or an application's configuration). REF: IA-2(1), AC-2(7) 800-53r5.	Functional	Intersects With	Phishing-Resistant Multi-Factor Authentication (MFA)	IAC-37.2	Automated mechanisms exist to enforce phishing-resistant Multi-Factor Authentication (MFA) through authenticators that are cryptographically bound to the verifier's identity, preventing credential relay by an impersonating party.	8		
5.3.6 / NSF2	N/A	Require phishing resistant MFA for all remote access. Protocols such as SSH, RDP (remote desktop), FTP, VNC, or VPN should require MFA. REF: IA-2(2), AC-17 800-53r5.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	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 (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	8		IAC-06
5.3.6 / NSF2	N/A	Require phishing resistant MFA for all remote access. Protocols such as SSH, RDP (remote desktop), FTP, VNC, or VPN should require MFA. REF: IA-2(2), AC-17 800-53r5.	Functional	Intersects With	Phishing-Resistant Multi-Factor Authentication (MFA)	IAC-37.2	Automated mechanisms exist to enforce phishing-resistant Multi-Factor Authentication (MFA) through authenticators that are cryptographically bound to	8		
5.3.6 / NSF2	N/A	Require phishing resistant MFA for all remote access. Protocols such as SSH, RDP (remote desktop), FTP, VNC, or VPN should require MFA. REF: IA-2(2), AC-17 800-53r5.	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		NET-14

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: USA - NSF Research Infrastructure Guide (January 2025) - Sections 5.2-5.3 (Cyberinfrastructure & Information Assurance)
Focal Document URL: https://www.nsf.gov/bfa/lfo/lfo_documents.jsp
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-nsf-rig-2025-information-assurance.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	Legacy SCF #
5.3.6 / NSF3	N/A	Limited scope administrative accounts: Privileged/administrative accounts should be restricted in scope (e.g., separate accounts for web servers, database servers, system management, network management). REF: AC-6(4,5), SC-3, CM-7 800-53r5; 3.1.5 800-171.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5		IAC-16
5.3.6 / NSF3	N/A	Limited scope administrative accounts: Privileged/administrative accounts should be restricted in scope (e.g., separate accounts for web servers, database servers, system management, network management). REF: AC-6(4,5), SC-3, CM-7 800-53r5; 3.1.5 800-171.	Functional	Intersects With	Least Privilege	IAC-30	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	5		IAC-21
5.3.6 / NSF3	N/A	Limited scope administrative accounts: Privileged/administrative accounts should be restricted in scope (e.g., separate accounts for web servers, database servers, system management, network management). REF: AC-6(4,5), SC-3, CM-7 800-53r5; 3.1.5 800-171.	Functional	Intersects With	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-30.1	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	5		IAC-21.5
5.3.6 / NSF4	N/A	Deploy and maintain anti-malware software to systems capable of running such software. Some systems (e.g., instrumentation, HPC, embedded systems, control systems) may not be able to run anti-malware software and are thus excluded from this control. REF: SI-3 800-53r5.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	8		END-04
5.3.6 / NSF5	N/A	Anti-malware includes Endpoint Detection Response functionality. Modern anti-malware products include or can be supplemented with EDR functionality, which greatly improves the ability to validate system integrity. REF: SI-3, SI-7(7).	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-09	Mechanisms exist to utilize Endpoint Detection & Response (EDR) capabilities to detect, investigate and respond to anomalous and/or malicious activity.	8		END-06.2
5.3.6 / NSF6	N/A	Immutable backups of systems: Backups of CI should be stored in a fashion as to be immutable from change, corruption, or deletion. REF: CP-4 800-53r5.	Functional	Subset Of	Resilient Data Backup Architecture	BCD-23	Mechanisms exist to maintain a secure, immutable backup architecture.	10		
5.3.6 / NSF6	N/A	Immutable backups of systems: Backups of CI should be stored in a fashion as to be immutable from change, corruption, or deletion. REF: CP-4 800-53r5.	Functional	Intersects With	Data Backups	BCD-24	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 satisfy Recovery Time	8		BCD-11
5.3.6 / NSF6	N/A	Immutable backups of systems: Backups of CI should be stored in a fashion as to be immutable from change, corruption, or deletion. REF: CP-4 800-53r5.	Functional	Intersects With	Data Backup Modification and/or Destruction	BCD-33	Mechanisms exist to restrict access to modify and/or delete data backups to only those privileged users with assigned data backup and recovery operations	5		BCD-11.10
5.3.6 / NSF7	N/A	Immutable backups of essential research data: Critical research data should be backed up and stored in a fashion to be immutable from change, corruption, or deletion. REF: CP-4 800-53r5.	Functional	Intersects With	Resilient Data Backup Architecture	BCD-23	Mechanisms exist to maintain a secure, immutable backup architecture.	8		
5.3.6 / NSF7	N/A	Immutable backups of essential research data: Critical research data should be backed up and stored in a fashion to be immutable from change, corruption, or deletion. REF: CP-4 800-53r5.	Functional	Intersects With	Data Backups	BCD-24	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 satisfy Recovery Time	8		BCD-11
5.3.6 / NSF7	N/A	Immutable backups of essential research data: Critical research data should be backed up and stored in a fashion to be immutable from change, corruption, or deletion. REF: CP-4 800-53r5.	Functional	Intersects With	Data Backup Modification and/or Destruction	BCD-33	Mechanisms exist to restrict access to modify and/or delete data backups to only those privileged users with assigned data backup and recovery operations	5		BCD-11.10
5.3.6 / NSF8	N/A	Regular tests of backup integrity and testing of restoration process: The backup program should include a step to test the integrity of and ability for large scale restoration of backups at least once a year. REF: CP-4, CP-10 800-53r5.	Functional	Intersects With	Restoration Integrity Verification	BCD-31.1	Mechanisms exist to verify the integrity of data backups and other restoration assets prior to using them for restoration.	5		BCD-13.1
5.3.6 / NSF8	N/A	Regular tests of backup integrity and testing of restoration process: The backup program should include a step to test the integrity of and ability for large scale restoration of backups at least once a year. REF: CP-4, CP-10 800-53r5.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	8		BCD-11.1
5.3.6 / NSF9	N/A	Collect and monitor all system logs: System and application activity logs for the CI should be centrally collected for the purposes of security monitoring and auditing. REF: AU-2, SI-4 800-53r5.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
5.3.6 / NSF9	N/A	Collect and monitor all system logs: System and application activity logs for the CI should be centrally collected for the purposes of security monitoring and auditing. REF: AU-2, SI-4 800-53r5.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	8		MON-02
5.3.6 / NSF10	N/A	Network segmentation and isolation control: The network environment should be segmented, reducing the ability of malware, such as ransomware, to spread. This may include any method of segmentation (e.g., network design and routing, internal firewalls, proxies, bastion hosts) sufficient to protect the infrastructure. REF: SC-7(13,20,21,28,29) 800-53r5; 3.13 800-171r2.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	8		NET-06
5.3.6 / NSF11	N/A	Maintain and update an inventory of critical infrastructure: systems and devices that maintain and provide access to services (e.g., VPN, MFA, Identity and Access Management systems), network devices, and devices enabling core scientific capabilities. REF: RA-2, PM-5 800-53r5.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8		AST-02
5.3.6 / NSF11	N/A	Maintain and update an inventory of critical infrastructure: systems and devices that maintain and provide access to services (e.g., VPN, MFA, Identity and Access Management systems), network devices, and devices enabling core scientific capabilities. REF: RA-2, PM-5 800-53r5.	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5		BCD-02
5.3.6 / NSF12	N/A	Defined process for identifying, tracking, and remediating vulnerabilities: A vulnerability management program is a framework for managing vulnerabilities in systems and software throughout the CI. REF: RA-5 800-53r5.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	8		VPM-01
5.3.6 / NSF12	N/A	Defined process for identifying, tracking, and remediating vulnerabilities: A vulnerability management program is a framework for managing vulnerabilities in systems and software throughout the CI. REF: RA-5 800-53r5.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
5.3.6 / NSF13	N/A	Hardening standards/processes for critical infrastructure: Create and implement a secure configuration standard applied to all systems under direct management. REF: CM-2, CM-6 800-53r5.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	8		CFG-02
5.3.6 / NSF14	N/A	Incident Response Plan and annual tabletop exercise simulating a major incident: Ensure the Incident Response Plan is documented and approved by Program and facility leadership. Run a regular tabletop exercise of it at least annually. REF: IR-2(1), IR-8, IR-3 800-53r5.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8		IRO-04
5.3.6 / NSF14	N/A	Incident Response Plan and annual tabletop exercise simulating a major incident: Ensure the Incident Response Plan is documented and approved by Program and facility leadership. Run a regular tabletop exercise of it at least annually. REF: IR-2(1), IR-8, IR-3 800-53r5.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06
5.3.7	Building an Information Assurance Program	A framework refers to the approach taken to organizing an IA Program. NSF does not require the use of any specific framework but requires Awardees to select one for their program and identify it in the IAMP; maintenance of a mapping to federal or international frameworks such as NIST CSF or ISO 27001/27002 is recommended. Four key elements upon which to build resilience: mission alignment, governance, resources, and cybersecurity controls.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	5		GOV-01

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

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **USA - NSF Research Infrastructure Guide (January 2025) - Sections 5.2-5.3 (Cyberinfrastructure & Information Assurance)**
Focal Document URL: https://www.nsf.gov/bfa/lfo/lfo_documents.jsp
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-nsf-rig-2025-information-assurance.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	Legecy SCF #
5.3.7	Building an Information Assurance Program	A framework refers to the approach taken to organizing an IA Program. NSF does not require the use of any specific framework but requires Awardees to select one for their program and identify it in the IAMP; maintenance of a mapping to federal or international frameworks such as NIST CSF or ISO 27001/27002 is recommended. Four key elements upon which to build resilience: mission alignment, governance, resources, and cybersecurity controls.	Functional	Intersects With	Select Controls	GOV-11.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15.1
5.3.7.1	N/A	Mission Alignment: requires understanding the scientific goals and workflows at a facility and considering the researchers' concerns in shaping the selection and implementation of practices, particularly in the early planning and pre-implementation stages of a facility.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	3		GOV-01
5.3.7.2	N/A	Governance: Oversight of IA is part of the overall facility governance process. Organizational roles, policies, the acceptance or mitigation of risk, and program assessment require engagement from the most senior administrators of a facility.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1
5.3.7.3	N/A	Resources: IA Programs require adequate resources. It is critical for an organization to be able to line item the IA budget, thus surfacing the investment for explicit review by management.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-05	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions.	5		PRM-02
5.3.7.3	N/A	Resources: IA Programs require adequate resources. It is critical for an organization to be able to line item the IA budget, thus surfacing the investment for explicit review by management.	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	5		PRM-03
5.3.7.4	N/A	Cybersecurity Controls: Every IA Program, within its IAMP, should identify a set of cybersecurity controls it plans to implement. NSF has identified a small set of essential security controls for prioritized implementation; these should be included as part of the identified baseline control set. NSF recommends selecting a baseline standard that includes practices that are widely established and offer the broadest protection (e.g., CISA Cross-Sector Cybersecurity Performance Goals, CIS Controls).	Functional	Intersects With	Select Controls	GOV-11.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15.1
5.3.8	Data Management and Curation	NSF recommends considering data management and cybersecurity holistically by reviewing access to data and data integrity concerns through the lens of cybersecurity. Facilities should perform a close analysis with researchers to identify data that should be retained, establish retention lifetimes, obtain DOIs, target repositories, and identify data sets for which data integrity and provenance concerns are paramount. Interfaces to data repositories should be examined as a possible entry vector for malicious activities and malware. IA staff can partner with domain scientists to make recommendations on secure data handling and access procedures.	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	5		DCH-01
5.3.8	Data Management and Curation	NSF recommends considering data management and cybersecurity holistically by reviewing access to data and data integrity concerns through the lens of cybersecurity. Facilities should perform a close analysis with researchers to identify data that should be retained, establish retention lifetimes, obtain DOIs, target repositories, and identify data sets for which data integrity and provenance concerns are paramount. Interfaces to data repositories should be examined as a possible entry vector for malicious activities and malware. IA staff can partner with domain scientists to make recommendations on secure data handling and access procedures.	Functional	Intersects With	Media & Data Retention	DCH-27	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	3		DCH-18
5.3.9	Information Assurance and Cyberinfrastructure	It is useful when writing an IAMP to consider how IA and CI relate to one another. CI is itself secured through the application of IA practices; however, because IA is fundamentally a risk management function, it should not be seen as exclusively a subset of a CI Plan. Strategies for cyber risk management should be articulated in the integrated risk program for the entire RI and referenced in the IAMP.	Functional	No Relationship	N/A	N/A	N/A	0		
5.3.10	Cyberbreach Insurance	Increasingly organizations, including Major Facilities, have obtained or are pursuing insurance to cover the costs associated with a cybersecurity incident. NSF neither requires, nor takes a position on, cyber breach insurance, however NSF recommends this as a discussion topic with the cognizant NSF PO. NSF policy dictates that award funds may not be used to pay ransoms, nor cyber insurance's ransom coverage.	Functional	No Relationship	N/A	N/A	N/A	0		
5.3.11	Program Assessment	NSF expects RI leadership or the managing organization to annually assess the effectiveness and progress of its IA Program in the context of reportable events and support of its mission. This can be achieved using internal or external assessors. During program review, evaluation covers: progress implementing the baseline controls set; whether mitigations identified in the Risk Register are successfully implemented; and whether significant, reportable incidents have been avoided. Over the life cycle, the IA Program should show steady improvement in maturity as measured using a commonly established	Functional	Intersects With	Conformity Monitoring	CPL-05	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5		CPL-03
5.3.11	Program Assessment	NSF expects RI leadership or the managing organization to annually assess the effectiveness and progress of its IA Program in the context of reportable events and support of its mission. This can be achieved using internal or external assessors. During program review, evaluation covers: progress implementing the baseline controls set; whether mitigations identified in the Risk Register are successfully implemented; and whether significant, reportable incidents have been avoided. Over the life cycle, the IA Program should show steady improvement in maturity as measured using a commonly established	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5		IAO-02