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 - DoW Brilliant at the Basics: Top 10 IT Cybersecurity Best Practices for DIB Partners**
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/Library/Brilliant-at-the-Basics_IT-Tipsv1.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-brilliant-basics-it.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 #
1	Phishing-Resistant Multi-Factor Authentication (MFA)	Upgrade your authentication mechanisms to require strong phishing-resistant MFA methods for user accounts. Moving away from legacy MFA methods such as SMS text messages or push notifications forms the foundation of a modern security stack. By combining explicit identity verification with least-privilege principles, you minimize the utility of compromised credentials and significantly reduce the risk of unauthorized access to sensitive systems.	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		
2	Comprehensive Asset Inventory Management	Establish and maintain a dynamically updated inventory of enterprise assets, including hardware, software, identities, and data across your estate. An effective inventory goes beyond a simple static list by providing a highly contextualized understanding of every asset. By continuously tracking and validating authorized assets with deep context, you establish the operational visibility required to detect anomalies, manage complex vulnerabilities, maintain compliance, and build a truly resilient defense.	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
2	Comprehensive Asset Inventory Management	Establish and maintain a dynamically updated inventory of enterprise assets, including hardware, software, identities, and data across your estate. An effective inventory goes beyond a simple static list by providing a highly contextualized understanding of every asset. By continuously tracking and validating authorized assets with deep context, you establish the operational visibility required to detect anomalies, manage complex vulnerabilities, maintain compliance, and build a truly resilient defense.	Functional	Intersects With	Comprehensive Asset Inventory Management	AST-08	Mechanisms exist to maintain a dynamically updated inventory of Technology Assets, Applications, Services and/or Data (TAASD) that provides a highly contextualized understanding of every asset that is capable of providing operational visibility required to: (1) Detect anomalies; (2) Manage complex vulnerabilities; (3) Maintain compliance; and (4) Maintain resilient capabilities.	5		
2	Comprehensive Asset Inventory Management	Establish and maintain a dynamically updated inventory of enterprise assets, including hardware, software, identities, and data across your estate. An effective inventory goes beyond a simple static list by providing a highly contextualized understanding of every asset. By continuously tracking and validating authorized assets with deep context, you establish the operational visibility required to detect anomalies, manage complex vulnerabilities, maintain compliance, and build a truly resilient defense.	Functional	Intersects With	User & Service Account Inventories	IAC-08.3	Mechanisms exist to maintain a current list of authorized users and service accounts.	5		IAC-01.3
3	Strategic Technical Debt Reduction	Minimize your attack surface by aggressively identifying, modernizing, consolidating, or retiring unused legacy infrastructure, redundant data stores, unsupported software, and unnecessary interfaces. Unmanaged "shadow IT" represents prime targets for adversarial exploitation and undermines modern zero-trust controls. Decommissioning these outdated technologies directly hardens your enterprise resilience, lowers operational complexity, and allows you to securely deploy capabilities at the speed of the mission.	Functional	Intersects With	Decommissioning	AST-36	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that: (1) Data is properly transitioned to new systems or archived; and (2) Hard drives are either destroyed or erased in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5		AST-30
3	Strategic Technical Debt Reduction	Minimize your attack surface by aggressively identifying, modernizing, consolidating, or retiring unused legacy infrastructure, redundant data stores, unsupported software, and unnecessary interfaces. Unmanaged "shadow IT" represents prime targets for adversarial exploitation and undermines modern zero-trust controls. Decommissioning these outdated technologies directly hardens your enterprise resilience, lowers operational complexity, and allows you to securely deploy capabilities at the speed of the mission.	Functional	Intersects With	Technical Debt Reviews	AST-38	Mechanisms exist to conduct ongoing "technical debt" reviews of hardware and software technologies to remediate outdated and/or unsupported technologies.	8		SEA-02.3
3	Strategic Technical Debt Reduction	Minimize your attack surface by aggressively identifying, modernizing, consolidating, or retiring unused legacy infrastructure, redundant data stores, unsupported software, and unnecessary interfaces. Unmanaged "shadow IT" represents prime targets for adversarial exploitation and undermines modern zero-trust controls. Decommissioning these outdated technologies directly hardens your enterprise resilience, lowers operational complexity, and allows you to securely deploy capabilities at the speed of the mission.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS 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 TAAS required to satisfy mission/business needs.	8		TDA-17
3	Strategic Technical Debt Reduction	Minimize your attack surface by aggressively identifying, modernizing, consolidating, or retiring unused legacy infrastructure, redundant data stores, unsupported software, and unnecessary interfaces. Unmanaged "shadow IT" represents prime targets for adversarial exploitation and undermines modern zero-trust controls. Decommissioning these outdated technologies directly hardens your enterprise resilience, lowers operational complexity, and allows you to securely deploy capabilities at the speed of the mission.	Functional	Intersects With	Shadow Information Technology Detection	OPS-09	Mechanisms exist to detect the presence of unauthorized Technology Assets, Applications and/or Services (TAAS) in use.	5		OPS-07
4	Flexible Technology Stack	Design and maintain a flexible, interoperable stack that supports modular integration of best-in-class commercial technologies. Prioritize open standards and solutions that facilitate interoperability and secure data exchange. Maintaining a modular architecture enables continuous operational agility and mitigates the strategic risk of being locked into a single proprietary vendor ecosystem.	Functional	Intersects With	Security, Compliance & Resilience Aware Design	SEA-02	Mechanisms exist to formally incorporate the organization's secure architecture principles into engineering, product and model design requirements to ensure security, compliance and resilience are built in by default and by design.	5		SEA-01.5
4	Flexible Technology Stack	Design and maintain a flexible, interoperable stack that supports modular integration of best-in-class commercial technologies. Prioritize open standards and solutions that facilitate interoperability and secure data exchange. Maintaining a modular architecture enables continuous operational agility and mitigates the strategic risk of being locked into a single proprietary vendor ecosystem.	Functional	Intersects With	Flexible Technology Stack	SEA-02.2	Mechanisms exist to design and maintain a flexible, interoperable stack that supports modular integration of best-in-class commercial Technology Assets, Applications and Services (TAAS).	5		
4	Flexible Technology Stack	Design and maintain a flexible, interoperable stack that supports modular integration of best-in-class commercial technologies. Prioritize open standards and solutions that facilitate interoperability and secure data exchange. Maintaining a modular architecture enables continuous operational agility and mitigates the strategic risk of being locked into a single proprietary vendor ecosystem.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-04	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	3		SEA-02
4	Flexible Technology Stack	Design and maintain a flexible, interoperable stack that supports modular integration of best-in-class commercial technologies. Prioritize open standards and solutions that facilitate interoperability and secure data exchange. Maintaining a modular architecture enables continuous operational agility and mitigates the strategic risk of being locked into a single proprietary vendor ecosystem.	Functional	Intersects With	Supplier Diversity	TPM-06	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	3		TDA-03.1
5	Logical Segmentation to Limit Adversary Lateral Movement	Implement software-defined segmentation to divide your environment into secure, isolated logical zones. Because adversaries actively attempt to move laterally to high-value targets once they gain initial access, flat networks pose a severe risk to sensitive data. Restricting lateral pathways limits the "blast radius" of any compromise and isolates sensitive Department data even if an individual endpoint is breached.	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	Logical Segmentation to Limit Adversary Lateral Movement	Implement software-defined segmentation to divide your environment into secure, isolated logical zones. Because adversaries actively attempt to move laterally to high-value targets once they gain initial access, flat networks pose a severe risk to sensitive data. Restricting lateral pathways limits the "blast radius" of any compromise and isolates sensitive Department data even if an individual endpoint is breached.	Functional	Intersects With	Microsegmentation	NET-11	Automated mechanisms exist to enable microsegmentation, either physically or virtually, to divide the network according to application and data workflows communications needs.	5		NET-06.6
6	Risk-Based Vulnerability Management	Establish a continuous, risk-based vulnerability management program driven by operational context and impact rather than generic severity scores. Replace flat patching cycles by prioritizing remediation actions based on the actual exploitability of a vulnerability, given your specific system configurations, existing compensating controls, and current operational state. Focusing on real operational risk aligns your limited resources to address the issues that matter most to your operations, security posture, and the broader mission.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	5		VPM-01
6	Risk-Based Vulnerability Management	Establish a continuous, risk-based vulnerability management program driven by operational context and impact rather than generic severity scores. Replace flat patching cycles by prioritizing remediation actions based on the actual exploitability of a vulnerability, given your specific system configurations, existing compensating controls, and current operational state. Focusing on real operational risk aligns your limited resources to address the issues that matter most to your operations, security posture, and the broader mission.	Functional	Intersects With	Attack Surface Scope	VPM-03	Mechanisms exist to define and manage the scope for its attack surface management activities.	3		VPM-01.1

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 - DoW Brilliant at the Basics: Top 10 IT Cybersecurity Best Practices for DIB Partners
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/Library/Brilliant-at-the-Basics_IT-Tipsv1.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-brilliant-basics-it.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 #
6	Risk-Based Vulnerability Management	Establish a continuous, risk-based vulnerability management program driven by operational context and impact rather than generic severity scores. Replace flat patching cycles by prioritizing remediation actions based on the actual exploitability of a vulnerability, given your specific system configurations, existing compensating controls, and current operational state. Focusing on real operational risk aligns your limited resources to address the issues that matter most to your operations, security posture, and the broader mission.	Functional	Intersects With	Vulnerability Exploitation Analysis	VPM-04	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	8		VPM-03.1
6	Risk-Based Vulnerability Management	Establish a continuous, risk-based vulnerability management program driven by operational context and impact rather than generic severity scores. Replace flat patching cycles by prioritizing remediation actions based on the actual exploitability of a vulnerability, given your specific system configurations, existing compensating controls, and current operational state. Focusing on real operational risk aligns your limited resources to address the issues that matter most to your operations, security posture, and the broader mission.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
6	Risk-Based Vulnerability Management	Establish a continuous, risk-based vulnerability management program driven by operational context and impact rather than generic severity scores. Replace flat patching cycles by prioritizing remediation actions based on the actual exploitability of a vulnerability, given your specific system configurations, existing compensating controls, and current operational state. Focusing on real operational risk aligns your limited resources to address the issues that matter most to your operations, security posture, and the broader mission.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8		VPM-02
6	Risk-Based Vulnerability Management	Establish a continuous, risk-based vulnerability management program driven by operational context and impact rather than generic severity scores. Replace flat patching cycles by prioritizing remediation actions based on the actual exploitability of a vulnerability, given your specific system configurations, existing compensating controls, and current operational state. Focusing on real operational risk aligns your limited resources to address the issues that matter most to your operations, security posture, and the broader mission.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-06.1	Mechanisms exist to centrally-manage the flaw remediation process.	5		VPM-05.1
6	Risk-Based Vulnerability Management	Establish a continuous, risk-based vulnerability management program driven by operational context and impact rather than generic severity scores. Replace flat patching cycles by prioritizing remediation actions based on the actual exploitability of a vulnerability, given your specific system configurations, existing compensating controls, and current operational state. Focusing on real operational risk aligns your limited resources to address the issues that matter most to your operations, security posture, and the broader mission.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-06.2	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5		VPM-04
6	Risk-Based Vulnerability Management	Establish a continuous, risk-based vulnerability management program driven by operational context and impact rather than generic severity scores. Replace flat patching cycles by prioritizing remediation actions based on the actual exploitability of a vulnerability, given your specific system configurations, existing compensating controls, and current operational state. Focusing on real operational risk aligns your limited resources to address the issues that matter most to your operations, security posture, and the broader mission.	Functional	Intersects With	Known Exploited Vulnerabilities (KEV) Mitigations	VPM-06.3	Mechanisms exist to prioritize remediation and mitigation of Known Exploited Vulnerabilities (KEV) by: (1) Reducing or removing public exposure to exploitation; and (2) Expediting patch deployment actions.	5		VPM-02.1
7	Integrate Security Early in the Development Lifecycle	Integrate secure coding standards and automated vulnerability scanning directly into the earliest phases of your engineering lifecycle. By shifting security left and testing software components, including all third-party dependencies, during the development phase, you are better positioned to deliver secure capabilities to the warfighter at speed and scale.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	8		PRM-07
7	Integrate Security Early in the Development Lifecycle	Integrate secure coding standards and automated vulnerability scanning directly into the earliest phases of your engineering lifecycle. By shifting security left and testing software components, including all third-party dependencies, during the development phase, you are better positioned to deliver secure capabilities to the warfighter at speed and scale.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	8		PRM-04
7	Integrate Security Early in the Development Lifecycle	Integrate secure coding standards and automated vulnerability scanning directly into the earliest phases of your engineering lifecycle. By shifting security left and testing software components, including all third-party dependencies, during the development phase, you are better positioned to deliver secure capabilities to the warfighter at speed and scale.	Functional	Subset Of	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10		TDA-06
7	Integrate Security Early in the Development Lifecycle	Integrate secure coding standards and automated vulnerability scanning directly into the earliest phases of your engineering lifecycle. By shifting security left and testing software components, including all third-party dependencies, during the development phase, you are better positioned to deliver secure capabilities to the warfighter at speed and scale.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	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.	8		TDA-09
8	Secure AI Adoption and Data Protection	Establish clear policies and technical guardrails governing the use of artificial intelligence and automation tools across your workforce. Explicitly prohibit the input of sensitive Department data into public, commercial AI systems. By implementing content filtering, endpoint controls, and approved enterprise AI environments, you prevent accidental data exposure while enabling the safe adoption of advanced technologies.	Functional	Subset Of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-02	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10		AAT-01
8	Secure AI Adoption and Data Protection	Establish clear policies and technical guardrails governing the use of artificial intelligence and automation tools across your workforce. Explicitly prohibit the input of sensitive Department data into public, commercial AI systems. By implementing content filtering, endpoint controls, and approved enterprise AI environments, you prevent accidental data exposure while enabling the safe adoption of advanced technologies.	Functional	Intersects With	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-18	Mechanisms exist to prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	3		AAT-12
8	Secure AI Adoption and Data Protection	Establish clear policies and technical guardrails governing the use of artificial intelligence and automation tools across your workforce. Explicitly prohibit the input of sensitive Department data into public, commercial AI systems. By implementing content filtering, endpoint controls, and approved enterprise AI environments, you prevent accidental data exposure while enabling the safe adoption of advanced technologies.	Functional	Intersects With	Sensitive / Regulated Data Governance	DCH-03	Mechanisms exist to facilitate data governance so that sensitive and/or regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5		GOV-10
8	Secure AI Adoption and Data Protection	Establish clear policies and technical guardrails governing the use of artificial intelligence and automation tools across your workforce. Explicitly prohibit the input of sensitive Department data into public, commercial AI systems. By implementing content filtering, endpoint controls, and approved enterprise AI environments, you prevent accidental data exposure while enabling the safe adoption of advanced technologies.	Functional	Intersects With	Rules of Behavior	HRS-06.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5		HRS-05.1
9	Resilient Backup and Disaster Recovery Architecture	Protect critical data from adversarial destruction and ransomware by establishing a secure, immutable backup architecture. Maintain redundant copies of all intellectual property, proprietary data, and Department records within a logically vaulted or offline environment. Ensure these backups are secure using isolated credentials distinct from your primary network, and enforce strict protections to prevent unauthorized modification or deletion. Regularly conduct full-system restoration drills to validate that your recovery pipelines can meet operational timelines in the event of a catastrophic compromise.	Functional	Intersects With	Isolated Recovery Environment	BCD-19	Mechanisms exist to utilize an isolated, non-production environment to perform data backup and recovery operations through offline, cloud or off-site capabilities.	5		BCD-14
9	Resilient Backup and Disaster Recovery Architecture	Protect critical data from adversarial destruction and ransomware by establishing a secure, immutable backup architecture. Maintain redundant copies of all intellectual property, proprietary data, and Department records within a logically vaulted or offline environment. Ensure these backups are secure using isolated credentials distinct from your primary network, and enforce strict protections to prevent unauthorized modification or deletion. Regularly conduct full-system restoration drills to validate that your recovery pipelines can meet operational timelines in the event of a catastrophic compromise.	Functional	Subset Of	Resilient Data Backup Architecture	BCD-23	Mechanisms exist to maintain a secure, immutable backup architecture.	10		

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 - DoW Brilliant at the Basics: Top 10 IT Cybersecurity Best Practices for DIB Partners**
Focal Document URL: https://dodcio.defense.gov/Portals/0/Documents/Library/Brilliant-at-the-Basics_IT-Tipsv1.pdf
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-brilliant-basics-it.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 #
9	Resilient Backup and Disaster Recovery Architecture	Protect critical data from adversarial destruction and ransomware by establishing a secure, immutable backup architecture. Maintain redundant copies of all intellectual property, proprietary data, and Department records within a logically vaulted or offline environment. Ensure these backups are secure using isolated credentials distinct from your primary network, and enforce strict protections to prevent unauthorized modification or deletion. Regularly conduct full-system restoration drills to validate that your recovery pipelines can meet operational timelines in the event of a catastrophic compromise.	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 Objectives (RTOs) and Recovery Point Objectives (RPOs).	8		BCD-11
9	Resilient Backup and Disaster Recovery Architecture	Protect critical data from adversarial destruction and ransomware by establishing a secure, immutable backup architecture. Maintain redundant copies of all intellectual property, proprietary data, and Department records within a logically vaulted or offline environment. Ensure these backups are secure using isolated credentials distinct from your primary network, and enforce strict protections to prevent unauthorized modification or deletion. Regularly conduct full-system restoration drills to validate that your recovery pipelines can meet operational timelines in the event of a catastrophic compromise.	Functional	Intersects With	Redundant Copies of Business-Critical Data	BCD-25	Mechanisms exist to maintain redundant copies of all business-critical data within one(1), or more, logically vaulted or offline environments.	8		
9	Resilient Backup and Disaster Recovery Architecture	Protect critical data from adversarial destruction and ransomware by establishing a secure, immutable backup architecture. Maintain redundant copies of all intellectual property, proprietary data, and Department records within a logically vaulted or offline environment. Ensure these backups are secure using isolated credentials distinct from your primary network, and enforce strict protections to prevent unauthorized modification or deletion. Regularly conduct full-system restoration drills to validate that your recovery pipelines can meet operational timelines in the event of a catastrophic compromise.	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.	5		BCD-11.1
9	Resilient Backup and Disaster Recovery Architecture	Protect critical data from adversarial destruction and ransomware by establishing a secure, immutable backup architecture. Maintain redundant copies of all intellectual property, proprietary data, and Department records within a logically vaulted or offline environment. Ensure these backups are secure using isolated credentials distinct from your primary network, and enforce strict protections to prevent unauthorized modification or deletion. Regularly conduct full-system restoration drills to validate that your recovery pipelines can meet operational timelines in the event of a catastrophic compromise.	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 roles.	5		BCD-11.10
10	Continuous Technical Workforce Readiness	Continuously develop your technical and security personnel on modern enterprise architecture, data protection, and defensive security operations. Operational resilience is directly bottlenecked by workforce capability. Prioritizing targeted technical training across your entire environment equips your team with the essential skills to defend sensitive information and counter evolving threats at the speed of the mission.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-02	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5		SAT-01
10	Continuous Technical Workforce Readiness	Continuously develop your technical and security personnel on modern enterprise architecture, data protection, and defensive security operations. Operational resilience is directly bottlenecked by workforce capability. Prioritizing targeted technical training across your entire environment equips your team with the essential skills to defend sensitive information and counter evolving threats at the speed of the mission.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8		SAT-03