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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
I	Executive Summary	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
I.A	N/A	Security Culture An institution's security culture contributes to the effectiveness of the information security program. The information security program is more effective when security processes are deeply embedded in the institution's culture. The board and management should understand and support information security and provide appropriate resources for developing, implementing, and maintaining the information security program. The result of this understanding and support is a program in which management and employees are committed to integrating the program into the institution's lines of business, support functions, and third-party management program. The introduction of new business initiatives (such as new service offerings or applications) can reveal the maturity of and degree to which information security is part of the institution's culture. An institution with a stronger security culture generally integrates information security into new initiatives from the outset and throughout the life cycles of services and applications. Another indicator of an effective culture is whether management and employees are held accountable for complying with the institution's	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	3		GOV-04.1
I.A	N/A	Security Culture An institution's security culture contributes to the effectiveness of the information security program. The information security program is more effective when security processes are deeply embedded in the institution's culture. The board and management should understand and support information security and provide appropriate resources for developing, implementing, and maintaining the information security program. The result of this understanding and support is a program in which management and employees are committed to integrating the program into the institution's lines of business, support functions, and third-party management program. The introduction of new business initiatives (such as new service offerings or applications) can reveal the maturity of and degree to which information security is part of the institution's culture. An institution with a stronger security culture generally integrates information security into new initiatives from the outset and throughout the life cycles of services and applications. Another indicator of an effective culture is whether management and employees are held accountable for complying with the institution's	Functional	Intersects With	Business As Usual (BAU) Security, Compliance & Resilience Practices	GOV-10	Mechanisms exist to incorporate security, compliance and resilience principles into Business As Usual (BAU) practices through executive leadership involvement.	5		GOV-14
I.A	N/A	Security Culture An institution's security culture contributes to the effectiveness of the information security program. The information security program is more effective when security processes are deeply embedded in the institution's culture. The board and management should understand and support information security and provide appropriate resources for developing, implementing, and maintaining the information security program. The result of this understanding and support is a program in which management and employees are committed to integrating the program into the institution's lines of business, support functions, and third-party management program. The introduction of new business initiatives (such as new service offerings or applications) can reveal the maturity of and degree to which information security is part of the institution's culture. An institution with a stronger security culture generally integrates information security into new initiatives from the outset and throughout the life cycles of services and applications. Another indicator of an effective culture is whether management and employees are held accountable for complying with the institution's	Functional	Intersects With	Risk Culture	RSK-04	Mechanisms exist to ensure teams are committed to a culture that considers and communicates technology-related risk.	5		RSK-12
I.B	N/A	Responsibility and Accountability The board, or designated board committee, should be responsible for overseeing the development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions. The board should reasonably understand the business case for information security and the business implications of information security risks; provide management with direction; approve information security plans, policies, and programs; review assessments of the information security program's effectiveness; and, when appropriate, discuss management's recommendations for corrective action. The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the information security program. The board, or designated board committee, should approve the institution's written information security program; affirm responsibilities for the development, implementation, and maintenance of the program; and review a report on the overall status of the program at least annually.7 Management should provide a report to the board at least annually8 that describes the overall status of the program and material matters related to the program, including the following: • Risk assessment process, including threat identification and assessment. • Risk management and control decisions, including risk acceptance and avoidance. • Third-party service provider arrangements. • Results of testing. • Security breaches or violations of law or regulation and management's responses to such incidents. • Recommendations for updates to the information security program. When providing reports on information security, management should include the results of management assessments and reviews; internal and external audit activity related to information security; third-party reviews of the information security program and information	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1
I.B	N/A	Responsibility and Accountability The board, or designated board committee, should be responsible for overseeing the development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions. The board should reasonably understand the business case for information security and the business implications of information security risks; provide management with direction; approve information security plans, policies, and programs; review assessments of the information security program's effectiveness; and, when appropriate, discuss management's recommendations for corrective action. The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the information security program. The board, or designated board committee, should approve the institution's written information security program; affirm responsibilities for the development, implementation, and maintenance of the program; and review a report on the overall status of the program at least annually.7 Management should provide a report to the board at least annually8 that describes the overall status of the program and material matters related to the program, including the following: • Risk assessment process, including threat identification and assessment. • Risk management and control decisions, including risk acceptance and avoidance. • Third-party service provider arrangements. • Results of testing. • Security breaches or violations of law or regulation and management's responses to such incidents. • Recommendations for updates to the information security program. When providing reports on information security, management should include the results of management assessments and reviews; internal and external audit activity related to information security; third-party reviews of the information security program and information	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
I.B	N/A	Responsibility and Accountability The board, or designated board committee, should be responsible for overseeing the development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions. The board should reasonably understand the business case for information security and the business implications of information security risks; provide management with direction; approve information security plans, policies, and programs; review assessments of the information security program's effectiveness; and, when appropriate, discuss management's recommendations for corrective action. The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the information security program. The board, or designated board committee, should approve the institution's written information security program; affirm responsibilities for the development, implementation, and maintenance of the program; and review a report on the overall status of the program at least annually.7 Management should provide a report to the board at least annually8 that describes the overall status of the program and material matters related to the program, including the following: • Risk assessment process, including threat identification and assessment. • Risk management and control decisions, including risk acceptance and avoidance. • Third-party service provider arrangements. • Results of testing. • Security breaches or violations of law or regulation and management's responses to such incidents. • Recommendations for updates to the information security program. When providing reports on information security, management should include the results of management assessments and reviews; internal and external audit activity related to information security; third-party reviews of the information security program and information	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).	5		GOV-04
I.B	N/A	Responsibility and Accountability The board, or designated board committee, should be responsible for overseeing the development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions. The board should reasonably understand the business case for information security and the business implications of information security risks; provide management with direction; approve information security plans, policies, and programs; review assessments of the information security program's effectiveness; and, when appropriate, discuss management's recommendations for corrective action. The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the information security program. The board, or designated board committee, should approve the institution's written information security program; affirm responsibilities for the development, implementation, and maintenance of the program; and review a report on the overall status of the program at least annually.7 Management should provide a report to the board at least annually8 that describes the overall status of the program and material matters related to the program, including the following: • Risk assessment process, including threat identification and assessment. • Risk management and control decisions, including risk acceptance and avoidance. • Third-party service provider arrangements. • Results of testing. • Security breaches or violations of law or regulation and management's responses to such incidents. • Recommendations for updates to the information security program. When providing reports on information security, management should include the results of management assessments and reviews; internal and external audit activity related to information security; third-party reviews of the information security program and information	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
I.B	N/A	Responsibility and Accountability The board, or designated board committee, should be responsible for overseeing the development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions. The board should reasonably understand the business case for information security and the business implications of information security risks; provide management with direction; approve information security plans, policies, and programs; review assessments of the information security program's effectiveness; and, when appropriate, discuss management's recommendations for corrective action. The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the information security program. The board, or designated board committee, should approve the institution's written information security program; affirm responsibilities for the development, implementation, and maintenance of the program; and review a report on the overall status of the program at least annually.7 Management should provide a report to the board at least annually8 that describes the overall status of the program and material matters related to the program, including the following: • Risk assessment process, including threat identification and assessment. • Risk management and control decisions, including risk acceptance and avoidance. • Third-party service provider arrangements. • Results of testing. • Security breaches or violations of law or regulation and management's responses to such incidents. • Recommendations for updates to the information security program. When providing reports on information security, management should include the results of management assessments and reviews; internal and external audit activity related to information security; third-party reviews of the information security program and information	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
I.B	N/A	Responsibility and Accountability The board, or designated board committee, should be responsible for overseeing the development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions. The board should reasonably understand the business case for information security and the business implications of information security risks; provide management with direction; approve information security plans, policies, and programs; review assessments of the information security program's effectiveness; and, when appropriate, discuss management's recommendations for corrective action. The board should provide management with its expectations and requirements and hold management accountable for central oversight and coordination, assignment of responsibility, and effectiveness of the information security program. The board, or designated board committee, should approve the institution's written information security program; affirm responsibilities for the development, implementation, and maintenance of the program; and review a report on the overall status of the program at least annually.7 Management should provide a report to the board at least annually8 that describes the overall status of the program and material matters related to the program, including the following: • Risk assessment process, including threat identification and assessment. • Risk management and control decisions, including risk acceptance and avoidance. • Third-party service provider arrangements. • Results of testing. • Security breaches or violations of law or regulation and management's responses to such incidents. • Recommendations for updates to the information security program. When providing reports on information security, management should include the results of management assessments and reviews; internal and external audit activity related to information security; third-party reviews of the information security program and information	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	3		HRS-11
I.C	N/A	Resources Funding, along with technical and managerial talent, also contributes to the effectiveness of the information security program. Management should provide, and the board should oversee, adequate funding to develop, implement, and maintain a successful information security program. The program should be staffed by sufficient personnel who have skills that are aligned with the institution's technical and managerial needs and commensurate with its size, complexity, and risk profile. Knowledge of technology standards, practices, and risk methodologies is particularly important to the success of the information security program. When third-party service providers supplement an institution's technical and managerial capabilities, management oversight should be commensurate with the sensitivity and criticality of the information and business processes supported by the third-party service provider. Refer to the IT Handbook's "Outsourcing Technology Services" booklet for more	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	5		HRS-03.2
I.C	N/A	Resources Funding, along with technical and managerial talent, also contributes to the effectiveness of the information security program. Management should provide, and the board should oversee, adequate funding to develop, implement, and maintain a successful information security program. The program should be staffed by sufficient personnel who have skills that are aligned with the institution's technical and managerial needs and commensurate with its size, complexity, and risk profile. Knowledge of technology standards, practices, and risk methodologies is particularly important to the success of the information security program. When third-party service providers supplement an institution's technical and managerial capabilities, management oversight should be commensurate with the sensitivity and criticality of the information and business processes supported by the third-party service provider. Refer to the IT Handbook's "Outsourcing Technology Services" booklet for more	Functional	Intersects With	Commitment To Continual Improvements	PRM-05.1	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	8		GOV-01.3
I.C	N/A	Resources Funding, along with technical and managerial talent, also contributes to the effectiveness of the information security program. Management should provide, and the board should oversee, adequate funding to develop, implement, and maintain a successful information security program. The program should be staffed by sufficient personnel who have skills that are aligned with the institution's technical and managerial needs and commensurate with its size, complexity, and risk profile. Knowledge of technology standards, practices, and risk methodologies is particularly important to the success of the information security program. When third-party service providers supplement an institution's technical and managerial capabilities, management oversight should be commensurate with the sensitivity and criticality of the information and business processes supported by the third-party service provider. Refer to the IT Handbook's "Outsourcing Technology Services" booklet for more	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
II	Introduction to Information Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.A	Risk Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.A.1	N/A	Threats According to the National Institute of Standards and Technology (NIST), a threat is any circumstance or event with the potential to create loss.12 A threat can be a natural occurrence, technology or physical failure, a person with intent to harm, or a person who unintentionally causes harm. Information about threats is available from public and private sources. Public sources include the news media, blogs, government publications and announcements, and various websites. Private sources include information security vendors and information-sharing organizations. The threat identification process is a means to collect data on potential threats that can assist management in its identification of information security risks. Threat modeling is a structured approach that enables an institution to aggregate and quantify potential threats. Institutions should consider using threat modeling to better understand the nature, frequency, and sophistication of threats; evaluate the information security risks to the institution; and apply this knowledge to the institution's information security program. As threats evolve rapidly, however, it is understood that modeling may not account for attacks that have not previously been seen, such as zero-day attacks, but could have significant	Functional	Intersects With	Threat Intelligence Feeds	THR-04	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5		THR-03
II.A.1	N/A	Threats According to the National Institute of Standards and Technology (NIST), a threat is any circumstance or event with the potential to create loss.12 A threat can be a natural occurrence, technology or physical failure, a person with intent to harm, or a person who unintentionally causes harm. Information about threats is available from public and private sources. Public sources include the news media, blogs, government publications and announcements, and various websites. Private sources include information security vendors and information-sharing organizations. The threat identification process is a means to collect data on potential threats that can assist management in its identification of information security risks. Threat modeling is a structured approach that enables an institution to aggregate and quantify potential threats. Institutions should consider using threat modeling to better understand the nature, frequency, and sophistication of threats; evaluate the information security risks to the institution; and apply this knowledge to the institution's information security program. As threats evolve rapidly, however, it is understood that modeling may not account for attacks that have not previously been seen, such as zero-day attacks, but could have significant	Functional	Intersects With	Threat Catalog	THR-06	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5		THR-09

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL:	https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL:	https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.A.1	N/A	Threats According to the National Institute of Standards and Technology (NIST), a threat is any circumstance or event with the potential to create loss.12 A threat can be a natural occurrence, technology or physical failure, a person with intent to harm, or a person who unintentionally causes harm. Information about threats is available from public and private sources. Public sources include the news media, blogs, government publications and announcements, and various websites. Private sources include information security vendors and information-sharing organizations. The threat identification process is a means to collect data on potential threats that can assist management in its identification of information security risks. Threat modeling is a structured approach that enables an institution to aggregate and quantify potential threats. Institutions should consider using threat modeling to better understand the nature, frequency, and sophistication of threats; evaluate the information security risks to the institution; and apply this knowledge to the institution's information security program. As threats evolve rapidly, however, it is understood that modeling may not account for attacks that have not previously been seen, such as zero-day attacks, but could have significant	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5		THR-10
II.A.2	N/A	Vulnerabilities A vulnerability is a weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source.13 A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation. These flaws provide opportunities for hackers to gain access to a computer system, execute commands as another user, or access data contrary to specified access restrictions. Institutions can use automated vulnerability scanners to scan their computer systems for known security exposures, as well as services available from third parties, such as the Mitre Corporation's Common Vulnerability and Exposures (CVE),14 to track vulnerabilities. In addition to technology-based vulnerabilities, weaknesses in business operational processes can create security vulnerabilities, exposing financial institutions to unwarranted risk. These vulnerabilities can include weaknesses in security procedures, administrative controls, physical layout, or internal controls that could be exploited to gain unauthorized access to information or to disrupt critical services. For example, an institution's systems architecture may be designed based on management's assumption that manual validation of wire transfers takes place before execution, when in practice the business process does not perform that validation until after transfers have taken place. 12 NIST SP (Special Publication) 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments," September 2012. 13 Ibid. 14 CVE is a dictionary of publicly known information security vulnerabilities and exposures. The Mitre Corporation maintains the system. CVE is sponsored by the U.S. Computer Emergency Readiness Team in the Office of Cybersecurity and Communications at the U.S. Department of Homeland Security. In addition to the vulnerabilities within a financial institution's system, vulnerabilities may also arise from	Functional	Intersects With	Risk Treatment Options	RSK-16.1	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance and service provider); or (4) Accepting the risk.	3		RSK-06.3
II.A.2	N/A	Vulnerabilities A vulnerability is a weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source.13 A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation. These flaws provide opportunities for hackers to gain access to a computer system, execute commands as another user, or access data contrary to specified access restrictions. Institutions can use automated vulnerability scanners to scan their computer systems for known security exposures, as well as services available from third parties, such as the Mitre Corporation's Common Vulnerability and Exposures (CVE),14 to track vulnerabilities. In addition to technology-based vulnerabilities, weaknesses in business operational processes can create security vulnerabilities, exposing financial institutions to unwarranted risk. These vulnerabilities can include weaknesses in security procedures, administrative controls, physical layout, or internal controls that could be exploited to gain unauthorized access to information or to disrupt critical services. For example, an institution's systems architecture may be designed based on management's assumption that manual validation of wire transfers takes place before execution, when in practice the business process does not perform that validation until after transfers have taken place. 12 NIST SP (Special Publication) 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments," September 2012. 13 Ibid. 14 CVE is a dictionary of publicly known information security vulnerabilities and exposures. The Mitre Corporation maintains the system. CVE is sponsored by the U.S. Computer Emergency Readiness Team in the Office of Cybersecurity and Communications at the U.S. Department of Homeland Security. In addition to the vulnerabilities within a financial institution's system, vulnerabilities may also arise from	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
II.A.2	N/A	Vulnerabilities A vulnerability is a weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source.13 A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation. These flaws provide opportunities for hackers to gain access to a computer system, execute commands as another user, or access data contrary to specified access restrictions. Institutions can use automated vulnerability scanners to scan their computer systems for known security exposures, as well as services available from third parties, such as the Mitre Corporation's Common Vulnerability and Exposures (CVE),14 to track vulnerabilities. In addition to technology-based vulnerabilities, weaknesses in business operational processes can create security vulnerabilities, exposing financial institutions to unwarranted risk. These vulnerabilities can include weaknesses in security procedures, administrative controls, physical layout, or internal controls that could be exploited to gain unauthorized access to information or to disrupt critical services. For example, an institution's systems architecture may be designed based on management's assumption that manual validation of wire transfers takes place before execution, when in practice the business process does not perform that validation until after transfers have taken place. 12 NIST SP (Special Publication) 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments," September 2012. 13 Ibid. 14 CVE is a dictionary of publicly known information security vulnerabilities and exposures. The Mitre Corporation maintains the system. CVE is sponsored by the U.S. Computer Emergency Readiness Team in the Office of Cybersecurity and Communications at the U.S. Department of Homeland Security. In addition to the vulnerabilities within a financial institution's system, vulnerabilities may also arise from	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.A.2	N/A	Vulnerabilities A vulnerability is a weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source.13 A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation. These flaws provide opportunities for hackers to gain access to a computer system, execute commands as another user, or access data contrary to specified access restrictions. Institutions can use automated vulnerability scanners to scan their computer systems for known security exposures, as well as services available from third parties, such as the Mitre Corporation's Common Vulnerability and Exposures (CVE),14 to track vulnerabilities. In addition to technology-based vulnerabilities, weaknesses in business operational processes can create security vulnerabilities, exposing financial institutions to unwarranted risk. These vulnerabilities can include weaknesses in security procedures, administrative controls, physical layout, or internal controls that could be exploited to gain unauthorized access to information or to disrupt critical services. For example, an institution's systems architecture may be designed based on management's assumption that manual validation of wire transfers takes place before execution, when in practice the business process does not perform that validation until after transfers have taken place. 12 NIST SP (Special Publication) 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments," September 2012. 13 Ibid. 14 CVE is a dictionary of publicly known information security vulnerabilities and exposures. The Mitre Corporation maintains the system. CVE is sponsored by the U.S. Computer Emergency Readiness Team in the Office of Cybersecurity and Communications at the U.S. Department of Homeland Security. In addition to the vulnerabilities within a financial institution's system, vulnerabilities may also arise from	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
II.A.3	Controls	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.A.3.a	N/A	Supervision of Cybersecurity Risk Cybersecurity is the process of protecting consumer and bank information by preventing, detecting, and responding to attacks. As part of cybersecurity, institutions should consider management of internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks. In light of the increasing volume and sophistication of cybersecurity threats, examiners should focus on cybersecurity preparedness in assessing the effectiveness of an institution's overall information security 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.	5		GOV-01
II.A.3.a	N/A	Supervision of Cybersecurity Risk Cybersecurity is the process of protecting consumer and bank information by preventing, detecting, and responding to attacks. As part of cybersecurity, institutions should consider management of internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks. In light of the increasing volume and sophistication of cybersecurity threats, examiners should focus on cybersecurity preparedness in assessing the effectiveness of an institution's overall information security program.	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
II.A.3.a	N/A	Supervision of Cybersecurity Risk Cybersecurity is the process of protecting consumer and bank information by preventing, detecting, and responding to attacks. As part of cybersecurity, institutions should consider management of internal and external threats and vulnerabilities to protect information assets and the supporting infrastructure from technology-based attacks. In light of the increasing volume and sophistication of cybersecurity threats, examiners should focus on cybersecurity preparedness in assessing the effectiveness of an institution's overall information security program.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	3		VPM-01
II.A.3.b	N/A	Resources for Cybersecurity Preparedness The FFIEC members issued a voluntary Cybersecurity Assessment Tool15 to help institution boards and management identify risks to their institutions and evaluate their institution's cybersecurity preparedness. In addition, there are other resources available to help management develop and evaluate information security and cyber resilience, such as the NIST Cybersecurity Framework, common approaches developed by the Mitre Corporation, and the U.S. Computer Emergency Readiness Team's (US-CERT)16 National Cyber Awareness System. Institution management can select a single framework or use a combination of resources to help identify its risks and determine its cybersecurity preparedness. Regardless of the source, frameworks can help management identify a cybersecurity and resilience posture that is commensurate with the institution's risk and complexity. 15 Refer to the Cybersecurity Assessment Tool on the FFIEC website. 16 US-CERT, of the Department of Homeland Security, responds to major incidents, analyzes threats, and exchanges critical cybersecurity information with trusted partners around the world.	Functional	Subset Of	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure practices.	10		GOV-01.4
II.B	N/A	Risk Measurement Action Summary Management should develop risk measurement processes that evaluate the inherent risk to the institution. The risk measurement process should be used to understand the institution's inherent risk and determine the risk associated with different threats. Management should use its measurement of the risks to guide its recommendations for and use of mitigating controls. Threat analysis tools assist in understanding and supporting the measurement of information security-related risks. Such tools can include event trees,17 attack trees,18 kill chains,19 and other security-related schemata.20 These tools help management deconstruct an event into stages, better understand the event, identify the most effective and efficient means of mitigating risk, and improve the information security program. Additionally, management could use a taxonomy for security-related events to help accomplish the following: • Map threats and vulnerabilities. • Incorporate legal and regulatory requirements. • Improve consistency in risk measurement. • Highlight potential areas for mitigation. • Select proper controls to cover various attack stages, channels, and assets. • Allow comparisons among different threats, events, and potential mitigating controls. Refer to the IT Handbook's "Management" booklet for more information. 17 An event tree is a diagram of a chronological series of events in a system or activity that displays sequence progression, end states, and dependencies across time. 18 An attack tree is a diagram showing how an asset, or target, might be attacked through various attack scenarios. Using an attack tree helps describe threats on computer systems and possible attacks to realize those threats. 19 A kill chain originally was used as a military concept related to the structure of an attack. In information security, a kill chain is a method for modeling intrusions on a computer network. 20 Security-related schemata are lists of software vulnerabilities and include the Mitre	Functional	Intersects With	Risk Assessment Methodology	RSK-12	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	5		RSK-04.2

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.B	N/A	Risk Measurement Action Summary Management should develop risk measurement processes that evaluate the inherent risk to the institution. The risk measurement process should be used to understand the institution's inherent risk and determine the risk associated with different threats. Management should use its measurement of the risks to guide its recommendations for and use of mitigating controls. Threat analysis tools assist in understanding and supporting the measurement of information security-related risks. Such tools can include event trees,17 attack trees,18 kill chains,19 and other security-related schemata.20 These tools help management deconstruct an event into stages, better understand the event, identify the most effective and efficient means of mitigating risk, and improve the information security program. Additionally, management could use a taxonomy for security-related events to help accomplish the following: • Map threats and vulnerabilities. • Incorporate legal and regulatory requirements. • Improve consistency in risk measurement. • Highlight potential areas for mitigation. • Select proper controls to cover various attack stages, channels, and assets. • Allow comparisons among different threats, events, and potential mitigating controls. Refer to the IT Handbook's "Management" booklet for more information. 17 An event tree is a diagram of a chronological series of events in a system or activity that displays sequence progression, end states, and dependencies across time. 18 An attack tree is a diagram showing how an asset, or target, might be attacked through various attack scenarios. Using an attack tree helps describe threats on computer systems and possible attacks to realize those threats. 19 A kill chain originally was used as a military concept related to the structure of an attack. In information security, a kill chain is a method for modeling intrusions on a computer network. 20 Security-related schemata are lists of software vulnerabilities and include the Mitre	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04
II.B	N/A	Risk Measurement Action Summary Management should develop risk measurement processes that evaluate the inherent risk to the institution. The risk measurement process should be used to understand the institution's inherent risk and determine the risk associated with different threats. Management should use its measurement of the risks to guide its recommendations for and use of mitigating controls. Threat analysis tools assist in understanding and supporting the measurement of information security-related risks. Such tools can include event trees,17 attack trees,18 kill chains,19 and other security-related schemata.20 These tools help management deconstruct an event into stages, better understand the event, identify the most effective and efficient means of mitigating risk, and improve the information security program. Additionally, management could use a taxonomy for security-related events to help accomplish the following: • Map threats and vulnerabilities. • Incorporate legal and regulatory requirements. • Improve consistency in risk measurement. • Highlight potential areas for mitigation. • Select proper controls to cover various attack stages, channels, and assets. • Allow comparisons among different threats, events, and potential mitigating controls. Refer to the IT Handbook's "Management" booklet for more information. 17 An event tree is a diagram of a chronological series of events in a system or activity that displays sequence progression, end states, and dependencies across time. 18 An attack tree is a diagram showing how an asset, or target, might be attacked through various attack scenarios. Using an attack tree helps describe threats on computer systems and possible attacks to realize those threats. 19 A kill chain originally was used as a military concept related to the structure of an attack. In information security, a kill chain is a method for modeling intrusions on a computer network. 20 Security-related schemata are lists of software vulnerabilities and include the Mitre	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5		THR-10
II.C	Information Security Program	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.C.1	N/A	Policies, Standards, and Procedures Information security policies, standards, and procedures should define the institution's control environment through a governance structure and provide descriptions of required, expected, and prohibited activities. Policies, standards, and procedures guide decisions and activities of users, developers, administrators, and managers and inform those individuals of their information security responsibilities. Policies, standards, and procedures should also specify the mechanisms through which responsibilities can be met. In addition, they should provide guidance on acquiring, designing, implementing, configuring, operating, maintaining, and auditing information systems. Policies, standards, and procedures that address the information security program should describe the roles of the information security department, lines of business, and IT organization in administering the information security program. Information security policies, standards, and procedures form the means by which the objectives of the information security program are achieved. Key attributes that contribute to the success of information security policies, standards, and procedures include the following: • Scope that describes the expectations for appropriate actions by affected parties. • Sufficient details to guide behavior. • Implementation through ordinary means, such as system administration procedures and acceptable use policies. • Enforcement through security tools and restrictions. • Delineation of the areas of responsibility for users, developers, administrators, and managers. • Clear and easily understandable communications to all affected parties. • Certification that employees have read and understand the policies. • Flexibility to address changes in the environment. • Annual board review and approval.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8		GOV-02
II.C.1	N/A	Policies, Standards, and Procedures Information security policies, standards, and procedures should define the institution's control environment through a governance structure and provide descriptions of required, expected, and prohibited activities. Policies, standards, and procedures guide decisions and activities of users, developers, administrators, and managers and inform those individuals of their information security responsibilities. Policies, standards, and procedures should also specify the mechanisms through which responsibilities can be met. In addition, they should provide guidance on acquiring, designing, implementing, configuring, operating, maintaining, and auditing information systems. Policies, standards, and procedures that address the information security program should describe the roles of the information security department, lines of business, and IT organization in administering the information security program. Information security policies, standards, and procedures form the means by which the objectives of the information security program are achieved. Key attributes that contribute to the success of information security policies, standards, and procedures include the following: • Scope that describes the expectations for appropriate actions by affected parties. • Sufficient details to guide behavior. • Implementation through ordinary means, such as system administration procedures and acceptable use policies. • Enforcement through security tools and restrictions. • Delineation of the areas of responsibility for users, developers, administrators, and managers. • Clear and easily understandable communications to all affected parties. • Certification that employees have read and understand the policies. • Flexibility to address changes in the environment. • Annual board review and approval.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5		GOV-03

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.1	N/A	Policies, Standards, and Procedures Information security policies, standards, and procedures should define the institution's control environment through a governance structure and provide descriptions of required, expected, and prohibited activities. Policies, standards, and procedures guide decisions and activities of users, developers, administrators, and managers and inform those individuals of their information security responsibilities. Policies, standards, and procedures should also specify the mechanisms through which responsibilities can be met. In addition, they should provide guidance on acquiring, designing, implementing, configuring, operating, maintaining, and auditing information systems. Policies, standards, and procedures that address the information security program should describe the roles of the information security department, lines of business, and IT organization in administering the information security program. Information security policies, standards, and procedures form the means by which the objectives of the information security program are achieved. Key attributes that contribute to the success of information security policies, standards, and procedures include the following: • Scope that describes the expectations for appropriate actions by affected parties. • Sufficient details to guide behavior. • Implementation through ordinary means, such as system administration procedures and acceptable use policies. • Enforcement through security tools and restrictions. • Delineation of the areas of responsibility for users, developers, administrators, and managers. • Clear and easily understandable communications to all affected parties. • Certification that employees have read and understand the policies. • Flexibility to address changes in the environment. • Annual board review and approval.	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-08.2	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	5		HRS-05.7
II.C.2	N/A	Technology Design While technology can introduce risk, it can also serve as a mitigation tool. Management should understand the benefits and limitations of the technology that the institution uses and whether other types of controls are necessary to compensate for those limitations. Information security issues arise when (a) the design of the technology and the policies governing its use do not effectively defend against identified and unidentified threats, (b) threats change in ways not envisioned by the designers, and (c) the controls are not operating as intended. Management should continually assess the capability of the institution's processes, people, and technologies to sustain the appropriate level of information security based on the institution's risk profile, size, complexity, and risk appetite.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	3		CPL-03.2
II.C.2	N/A	Technology Design While technology can introduce risk, it can also serve as a mitigation tool. Management should understand the benefits and limitations of the technology that the institution uses and whether other types of controls are necessary to compensate for those limitations. Information security issues arise when (a) the design of the technology and the policies governing its use do not effectively defend against identified and unidentified threats, (b) threats change in ways not envisioned by the designers, and (c) the controls are not operating as intended. Management should continually assess the capability of the institution's processes, people, and technologies to sustain the appropriate level of information security based on the institution's risk profile, size, complexity, and risk appetite.	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.	5		RSK-06.2
II.C.2	N/A	Technology Design While technology can introduce risk, it can also serve as a mitigation tool. Management should understand the benefits and limitations of the technology that the institution uses and whether other types of controls are necessary to compensate for those limitations. Information security issues arise when (a) the design of the technology and the policies governing its use do not effectively defend against identified and unidentified threats, (b) threats change in ways not envisioned by the designers, and (c) the controls are not operating as intended. Management should continually assess the capability of the institution's processes, people, and technologies to sustain the appropriate level of information security based on the institution's risk profile, size, complexity, and risk appetite.	Functional	Intersects With	Secure Engineering Principles	SEA-05	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).	5		SEA-01
II.C.3	N/A	Control Types Management may mitigate information security risks by implementing controls. Controls may be categorized according to timing and nature. Table 1: Examples of Timing- and Nature-Related Controls Timing Control type Description Example Preventive Controls designed to prevent incidents from occurring Access controls to applications and systems that prevent unauthorized individuals from performing transactions Detective Controls designed to alert management when incidents occur Reports that show suspicious activity Corrective Controls that lessen impact to the institution when adverse incidents occur Business continuity plans Nature Control type Description Example Administrative Controls that align with the board- approved risk appetite and inform employees of management's expectations Policies or procedures that guide implementation of the information security program Technical Software or hardware (or both) that prevents unauthorized activity A firewall that prevents unauthorized logical access to or from a network Physical Devices to prevent unauthorized physical access to a facility or computer system A deadbolt lock on a door It is important to have a layered control system, which deploys different controls at different points of a business process and throughout an IT system so that the strength of one control can compensate for weaknesses in or possible failure of another control. Therefore, layered controls function in an integrated fashion to more effectively mitigate risk. Economic and technical considerations generally affect prevention and detection or response choices in system design. Compensating controls are controls that adjust for weaknesses within the system or process. An example of compensating controls would be a review of activity logs for applications that do not allow proper segregation of duties.	Functional	Intersects With	Control Objectives	GOV-03.3	Mechanisms exist to establish control objectives as the basis for the design, selection, implementation and management of the organization's internal security, compliance and resilience control system.	3		GOV-09

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.3	N/A	Control Types Management may mitigate information security risks by implementing controls. Controls may be categorized according to timing and nature. Table 1: Examples of Timing- and Nature-Related Controls Timing Control type Description Example Preventive Controls designed to prevent incidents from occurring Access controls to applications and systems that prevent unauthorized individuals from performing transactions Detective Controls designed to alert management when incidents occur Reports that show suspicious activity Corrective Controls that lessen impact to the institution when adverse incidents occur Business continuity plans Nature Control type Description Example Administrative Controls that align with the board- approved risk appetite and inform employees of management's expectations Policies or procedures that guide implementation of the information security program Technical Software or hardware (or both) that prevents unauthorized activity A firewall that prevents unauthorized logical access to or from a network Physical Devices to prevent unauthorized physical access to a facility or computer system A deadbolt lock on a door It is important to have a layered control system, which deploys different controls at different points of a business process and throughout an IT system so that the strength of one control can compensate for weaknesses in or possible failure of another control. Therefore, layered controls function in an integrated fashion to more effectively mitigate risk. Economic and technical considerations generally affect prevention and detection or response choices in system design. Compensating controls are controls that adjust for weaknesses within the system or process. An example of compensating controls would be a review of activity logs for applications that do not allow proper segregation of duties.	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.	5		RSK-06.2
II.C.3	N/A	Control Types Management may mitigate information security risks by implementing controls. Controls may be categorized according to timing and nature. Table 1: Examples of Timing- and Nature-Related Controls Timing Control type Description Example Preventive Controls designed to prevent incidents from occurring Access controls to applications and systems that prevent unauthorized individuals from performing transactions Detective Controls designed to alert management when incidents occur Reports that show suspicious activity Corrective Controls that lessen impact to the institution when adverse incidents occur Business continuity plans Nature Control type Description Example Administrative Controls that align with the board- approved risk appetite and inform employees of management's expectations Policies or procedures that guide implementation of the information security program Technical Software or hardware (or both) that prevents unauthorized activity A firewall that prevents unauthorized logical access to or from a network Physical Devices to prevent unauthorized physical access to a facility or computer system A deadbolt lock on a door It is important to have a layered control system, which deploys different controls at different points of a business process and throughout an IT system so that the strength of one control can compensate for weaknesses in or possible failure of another control. Therefore, layered controls function in an integrated fashion to more effectively mitigate risk. Economic and technical considerations generally affect prevention and detection or response choices in system design. Compensating controls are controls that adjust for weaknesses within the system or process. An example of compensating controls would be a review of activity logs for applications that do not allow proper segregation of duties.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-06	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		SEA-03
II.C.4	N/A	Control Implementation Management should implement controls that align security with the nature of the institution's operations and strategic direction. Based on the institution's risk assessment, the controls should include, but may not be limited to, patch management, asset and configuration management, vulnerability scanning and penetration testing, end-point security, resilience controls, logging and monitoring, and secure software development (including third-party software development). In implementing controls, management should ensure it has the necessary resources, personnel training, and testing to maximize the effectiveness of the controls. The level at which controls are implemented should depend on the institution's size, complexity, and risk profile, but all institutions should implement appropriate controls. In light of increasing cybersecurity risks, management should implement risk-based controls for managing cybersecurity threats and vulnerabilities, such as interconnectivity risk. Management should review and update the security controls as necessary depending on changes to the internal and external operating environment, technologies, business processes, and other factors. The institution can reference one or more recognized technology frameworks and industry standards. Several organizations have published control listings in addition to implementation guidance, including the following: • NIST 800 series of publications. These publications provide descriptions of some management processes and technical guidance on many individual controls. • Control Objectives for Information and Related Technology (COBIT). COBIT provides a broad and deep framework for governance and management of enterprise IT. • IT Infrastructure Library (ITIL). ITIL provides a list of recognized practices for IT service management. • International Organization for Standardization (ISO)21 27000 series. The ISO 27000 series provides control standards specific to	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure practices.	5		GOV-01.4
II.C.4	N/A	Control Implementation Management should implement controls that align security with the nature of the institution's operations and strategic direction. Based on the institution's risk assessment, the controls should include, but may not be limited to, patch management, asset and configuration management, vulnerability scanning and penetration testing, end-point security, resilience controls, logging and monitoring, and secure software development (including third-party software development). In implementing controls, management should ensure it has the necessary resources, personnel training, and testing to maximize the effectiveness of the controls. The level at which controls are implemented should depend on the institution's size, complexity, and risk profile, but all institutions should implement appropriate controls. In light of increasing cybersecurity risks, management should implement risk-based controls for managing cybersecurity threats and vulnerabilities, such as interconnectivity risk. Management should review and update the security controls as necessary depending on changes to the internal and external operating environment, technologies, business processes, and other factors. The institution can reference one or more recognized technology frameworks and industry standards. Several organizations have published control listings in addition to implementation guidance, including the following: • NIST 800 series of publications. These publications provide descriptions of some management processes and technical guidance on many individual controls. • Control Objectives for Information and Related Technology (COBIT). COBIT provides a broad and deep framework for governance and management of enterprise IT. • IT Infrastructure Library (ITIL). ITIL provides a list of recognized practices for IT service management. • International Organization for Standardization (ISO)21 27000 series. The ISO 27000 series provides control standards specific to	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	3		GOV-03

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL:	https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL:	https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.4	N/A	Control Implementation Management should implement controls that align security with the nature of the institution's operations and strategic direction. Based on the institution's risk assessment, the controls should include, but may not be limited to, patch management, asset and configuration management, vulnerability scanning and penetration testing, end-point security, resilience controls, logging and monitoring, and secure software development (including third-party software development). In implementing controls, management should ensure it has the necessary resources, personnel training, and testing to maximize the effectiveness of the controls. The level at which controls are implemented should depend on the institution's size, complexity, and risk profile, but all institutions should implement appropriate controls. In light of increasing cybersecurity risks, management should implement risk-based controls for managing cybersecurity threats and vulnerabilities, such as interconnectivity risk. Management should review and update the security controls as necessary depending on changes to the internal and external operating environment, technologies, business processes, and other factors. The institution can reference one or more recognized technology frameworks and industry standards. Several organizations have published control listings in addition to implementation guidance, including the following: • NIST 800 series of publications. These publications provide descriptions of some management processes and technical guidance on many individual controls. • Control Objectives for Information and Related Technology (COBIT). COBIT provides a broad and deep framework for governance and management of enterprise IT. • IT Infrastructure Library (ITIL). ITIL provides a list of recognized practices for IT service management. • International Organization for Standardization (ISO)21 27000 series. The ISO 27000 series provides control standards specific to	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
II.C.4	N/A	Control Implementation Management should implement controls that align security with the nature of the institution's operations and strategic direction. Based on the institution's risk assessment, the controls should include, but may not be limited to, patch management, asset and configuration management, vulnerability scanning and penetration testing, end-point security, resilience controls, logging and monitoring, and secure software development (including third-party software development). In implementing controls, management should ensure it has the necessary resources, personnel training, and testing to maximize the effectiveness of the controls. The level at which controls are implemented should depend on the institution's size, complexity, and risk profile, but all institutions should implement appropriate controls. In light of increasing cybersecurity risks, management should implement risk-based controls for managing cybersecurity threats and vulnerabilities, such as interconnectivity risk. Management should review and update the security controls as necessary depending on changes to the internal and external operating environment, technologies, business processes, and other factors. The institution can reference one or more recognized technology frameworks and industry standards. Several organizations have published control listings in addition to implementation guidance, including the following: • NIST 800 series of publications. These publications provide descriptions of some management processes and technical guidance on many individual controls. • Control Objectives for Information and Related Technology (COBIT). COBIT provides a broad and deep framework for governance and management of enterprise IT. • IT Infrastructure Library (ITIL). ITIL provides a list of recognized practices for IT service management. • International Organization for Standardization (ISO)21 27000 series. The ISO 27000 series provides control standards specific to	Functional	Intersects With	Implement Controls	GOV-11.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15.2
II.C.5	N/A	Inventory and Classification of Assets Action Summary Management should inventory and classify assets, including hardware, software, information, and connections. Management should maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware, software, information, and connections. Management should have policies to govern the inventory and classification of assets both at inception and throughout their life cycle, and wherever the assets are stored, transmitted, or processed. Inventories enable management and staff to identify assets and their functions. Classification enables the institution to determine the sensitivity and criticality of assets. Management should use this classification to implement controls required to safeguard the institution's physical and information assets. Additionally, management can use the inventory to discover specific vulnerabilities, such as unauthorized software. Inventories are important for management to identify assets that require additional protection, such as those that store, transmit, or process sensitive customer information, trade secrets, or other information or assets that could be a target of cyber criminals. Knowing what information assets the institution has and where they are stored, transmitted, or processed helps management comply with federal and state laws and regulations regarding privacy and security of sensitive customer information. After inventorying the assets, management should classify the information according to the appropriate level of protection needed. For example, systems containing sensitive customer information may require access controls based on job responsibilities. These systems should have stronger controls than systems containing information meant for the general public. Some institutions classify information as public, non-public, or institution-confidential, while others use the classifications high, moderate, and	Functional	Intersects With	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5		AST-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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.5	N/A	Inventory and Classification of Assets Action Summary Management should inventory and classify assets, including hardware, software, information, and connections. Management should maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware, software, information, and connections. Management should have policies to govern the inventory and classification of assets both at inception and throughout their life cycle, and wherever the assets are stored, transmitted, or processed. Inventories enable management and staff to identify assets and their functions. Classification enables the institution to determine the sensitivity and criticality of assets. Management should use this classification to implement controls required to safeguard the institution's physical and information assets. Additionally, management can use the inventory to discover specific vulnerabilities, such as unauthorized software. Inventories are important for management to identify assets that require additional protection, such as those that store, transmit, or process sensitive customer information, trade secrets, or other information or assets that could be a target of cyber criminals. Knowing what information assets the institution has and where they are stored, transmitted, or processed helps management comply with federal and state laws and regulations regarding privacy and security of sensitive customer information. After inventorying the assets, management should classify the information according to the appropriate level of protection needed. For example, systems containing sensitive customer information may require access controls based on job responsibilities. These systems should have stronger controls than systems containing information meant for the general public. Some institutions classify information as public, non-public, or institution-confidential, while others use the classifications high, moderate, and	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
II.C.5	N/A	Inventory and Classification of Assets Action Summary Management should inventory and classify assets, including hardware, software, information, and connections. Management should maintain and keep updated an inventory of technology assets that classifies the sensitivity and criticality of those assets, including hardware, software, information, and connections. Management should have policies to govern the inventory and classification of assets both at inception and throughout their life cycle, and wherever the assets are stored, transmitted, or processed. Inventories enable management and staff to identify assets and their functions. Classification enables the institution to determine the sensitivity and criticality of assets. Management should use this classification to implement controls required to safeguard the institution's physical and information assets. Additionally, management can use the inventory to discover specific vulnerabilities, such as unauthorized software. Inventories are important for management to identify assets that require additional protection, such as those that store, transmit, or process sensitive customer information, trade secrets, or other information or assets that could be a target of cyber criminals. Knowing what information assets the institution has and where they are stored, transmitted, or processed helps management comply with federal and state laws and regulations regarding privacy and security of sensitive customer information. After inventorying the assets, management should classify the information according to the appropriate level of protection needed. For example, systems containing sensitive customer information may require access controls based on job responsibilities. These systems should have stronger controls than systems containing information meant for the general public. Some institutions classify information as public, non-public, or institution-confidential, while others use the classifications high, moderate, and	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02
II.C.6	N/A	Mitigating Interconnectivity Risk Business processes often require institutions to share information with other institutions and third-party service providers that require connectivity. The extent of interconnectivity is a function of network architecture, network complexity, traffic volume, and number of connections. Interconnectivity risk arises from misuse, mismanagement, or compromise of these connections. To mitigate interconnectivity risk, management should do the following: • Identify connections with third parties, including other financial institutions, financial institution intermediaries, and third-party service providers. • Identify all access points and connection types that pose risk, such as local area network (LAN) connections to other networks or Internet service providers (ISP), Wi-Fi, and cellular connections. • Identify connections between and access across low-risk and high-risk systems. • Assess all connections with third parties that provide remote access capability or control over internal systems. • Implement and assess the adequacy of controls to ensure the security of connections regardless of criticality or sensitivity. Management should maintain network and connectivity diagrams and data flow charts to ensure adequacy of layered controls and to facilitate more timely recovery and restoration of systems when	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AST-04
II.C.6	N/A	Mitigating Interconnectivity Risk Business processes often require institutions to share information with other institutions and third-party service providers that require connectivity. The extent of interconnectivity is a function of network architecture, network complexity, traffic volume, and number of connections. Interconnectivity risk arises from misuse, mismanagement, or compromise of these connections. To mitigate interconnectivity risk, management should do the following: • Identify connections with third parties, including other financial institutions, financial institution intermediaries, and third-party service providers. • Identify all access points and connection types that pose risk, such as local area network (LAN) connections to other networks or Internet service providers (ISP), Wi-Fi, and cellular connections. • Identify connections between and access across low-risk and high-risk systems. • Assess all connections with third parties that provide remote access capability or control over internal systems. • Implement and assess the adequacy of controls to ensure the security of connections regardless of criticality or sensitivity. Management should maintain network and connectivity diagrams and data flow charts to ensure adequacy of layered controls and to facilitate more timely recovery and restoration of systems when	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	5		NET-05

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.6	N/A	Mitigating Interconnectivity Risk Business processes often require institutions to share information with other institutions and third-party service providers that require connectivity. The extent of interconnectivity is a function of network architecture, network complexity, traffic volume, and number of connections. Interconnectivity risk arises from misuse, mismanagement, or compromise of these connections. To mitigate interconnectivity risk, management should do the following: • Identify connections with third parties, including other financial institutions, financial institution intermediaries, and third-party service providers. • Identify all access points and connection types that pose risk, such as local area network (LAN) connections to other networks or Internet service providers (ISP), Wi-Fi, and cellular connections. • Identify connections between and access across low-risk and high-risk systems. • Assess all connections with third parties that provide remote access capability or control over internal systems. • Implement and assess the adequacy of controls to ensure the security of connections regardless of criticality or sensitivity. Management should maintain network and connectivity diagrams and data flow charts to ensure adequacy of layered controls and to facilitate more timely recovery and restoration of systems when	Functional	Intersects With	External System Connections	NET-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.	5		NET-05.1
II.C.6	N/A	Mitigating Interconnectivity Risk Business processes often require institutions to share information with other institutions and third-party service providers that require connectivity. The extent of interconnectivity is a function of network architecture, network complexity, traffic volume, and number of connections. Interconnectivity risk arises from misuse, mismanagement, or compromise of these connections. To mitigate interconnectivity risk, management should do the following: • Identify connections with third parties, including other financial institutions, financial institution intermediaries, and third-party service providers. • Identify all access points and connection types that pose risk, such as local area network (LAN) connections to other networks or Internet service providers (ISP), Wi-Fi, and cellular connections. • Identify connections between and access across low-risk and high-risk systems. • Assess all connections with third parties that provide remote access capability or control over internal systems. • Implement and assess the adequacy of controls to ensure the security of connections regardless of criticality or sensitivity. Management should maintain network and connectivity diagrams and data flow charts to ensure adequacy of layered controls and to facilitate more timely recovery and restoration of systems when	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-04
II.C.7	Logical and Physical Access Controls	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.C.7.a	N/A	Security Screening in Hiring Practices Management should have a process to verify job application information for all new employees. The sensitivity of a particular job or access level may warrant additional screening and recurring background and credit checks. Management should verify that contractors are subject to similar screening procedures. In addition to initial screening, management should remain alert to changes in personal circumstances of employees and contractors that could increase incentives for system	Functional	Intersects With	Position Categorization	HRS-03	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5		HRS-02
II.C.7.a	N/A	Security Screening in Hiring Practices Management should have a process to verify job application information for all new employees. The sensitivity of a particular job or access level may warrant additional screening and recurring background and credit checks. Management should verify that contractors are subject to similar screening procedures. In addition to initial screening, management should remain alert to changes in personal circumstances of employees and contractors that could increase incentives for system	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	8		HRS-04
II.C.7.a	N/A	Security Screening in Hiring Practices Management should have a process to verify job application information for all new employees. The sensitivity of a particular job or access level may warrant additional screening and recurring background and credit checks. Management should verify that contractors are subject to similar screening procedures. In addition to initial screening, management should remain alert to changes in personal circumstances of employees and contractors that could increase incentives for system	Functional	Intersects With	Roles With Special Protection Measures	HRS-05.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5		HRS-04.1
II.C.7.a	N/A	Security Screening in Hiring Practices Management should have a process to verify job application information for all new employees. The sensitivity of a particular job or access level may warrant additional screening and recurring background and credit checks. Management should verify that contractors are subject to similar screening procedures. In addition to initial screening, management should remain alert to changes in personal circumstances of employees and contractors that could increase incentives for system	Functional	Intersects With	Third-Party Personnel	HRS-13	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	3		HRS-10
II.C.7.b	N/A	User Access Program Management should develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology. This program should include the following elements: • Principle of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity. • Alignment of employee job descriptions to the user access program. • Requirements for business and application owners to define user profiles. • Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel. • Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations. • Periodic independent reviews that ensure effective administration of user access, both physical and logical. For more information, refer to the "Physical Security" and "Logical Security" sections of this booklet.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
II.C.7.b	N/A	User Access Program Management should develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology. This program should include the following elements: • Principle of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity. • Alignment of employee job descriptions to the user access program. • Requirements for business and application owners to define user profiles. • Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel. • Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations. • Periodic independent reviews that ensure effective administration of user access, both physical and logical. For more information, refer to the "Physical Security" and "Logical Security" sections of this booklet.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-04	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5		IAC-07

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.7.b	N/A	User Access Program Management should develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology. This program should include the following elements: • Principle of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity. • Alignment of employee job descriptions to the user access program. • Requirements for business and application owners to define user profiles. • Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel. • Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations. • Periodic independent reviews that ensure effective administration of user access, both physical and logical. For more information, refer to the "Physical Security" and "Logical Security" sections of this booklet.	Functional	Intersects With	Change of Roles & Duties	IAC-04.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5		IAC-07.1
II.C.7.b	N/A	User Access Program Management should develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology. This program should include the following elements: • Principle of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity. • Alignment of employee job descriptions to the user access program. • Requirements for business and application owners to define user profiles. • Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel. • Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations. • Periodic independent reviews that ensure effective administration of user access, both physical and logical. For more information, refer to the "Physical Security" and "Logical Security" sections of this booklet.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5		IAC-17
II.C.7.b	N/A	User Access Program Management should develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology. This program should include the following elements: • Principle of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity. • Alignment of employee job descriptions to the user access program. • Requirements for business and application owners to define user profiles. • Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel. • Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations. • Periodic independent reviews that ensure effective administration of user access, both physical and logical. For more information, refer to the "Physical Security" and "Logical Security" sections of this booklet.	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 functions.	5		IAC-21
II.C.7.b	N/A	User Access Program Management should develop a user access program to implement and administer physical and logical access controls to safeguard the institution's information assets and technology. This program should include the following elements: • Principle of least privilege, which recommends minimum user profile privileges for both physical and logical access based on job necessity. • Alignment of employee job descriptions to the user access program. • Requirements for business and application owners to define user profiles. • Ongoing reviews by business line and application owners to verify appropriate access based on job roles with changes reported on a timely basis to security administration personnel. • Timely notification from human resources to security administrators to adjust user access based on job changes, including terminations. • Periodic independent reviews that ensure effective administration of user access, both physical and logical. For more information, refer to the "Physical Security" and "Logical Security" sections of this booklet.	Functional	Intersects With	Physical Access Authorizations	PES-06	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	3		PES-02
II.C.7.c	N/A	Segregation of Duties Segregation of duties, or job designs that require more than one person to complete critical or sensitive tasks, can help mitigate risk. Employees and third parties with access to sensitive resources could cause substantial damage and potential loss. System administrators, for instance, have the most powerful role in the user access process and have unlimited access to an institution's information assets and technology. Given this extensive access, management should evaluate the process for determining which individuals should be granted system administrator privileges. Such access should be appropriately monitored for unauthorized or inappropriate activity. Management should incorporate independent reviews or approvals for individuals who perform multiple functions to minimize the potential for fraud, irregularities, and errors. Examples of segregation of duties include the following: • Independent monitoring of the activities performed by the users with increased privileges (e.g., system administrators and super users23). • Distribution of system administration activities so no administrator can hide his or her activities or control an entire system. • Additional levels of approval as the criticality and sensitivity of decisions increase. If an activity is conducted without appropriate segregation of duties, management should require an independent review (e.g., audit) of that activity.	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	8		HRS-11
II.C.7.c	N/A	Segregation of Duties Segregation of duties, or job designs that require more than one person to complete critical or sensitive tasks, can help mitigate risk. Employees and third parties with access to sensitive resources could cause substantial damage and potential loss. System administrators, for instance, have the most powerful role in the user access process and have unlimited access to an institution's information assets and technology. Given this extensive access, management should evaluate the process for determining which individuals should be granted system administrator privileges. Such access should be appropriately monitored for unauthorized or inappropriate activity. Management should incorporate independent reviews or approvals for individuals who perform multiple functions to minimize the potential for fraud, irregularities, and errors. Examples of segregation of duties include the following: • Independent monitoring of the activities performed by the users with increased privileges (e.g., system administrators and super users23). • Distribution of system administration activities so no administrator can hide his or her activities or control an entire system. • Additional levels of approval as the criticality and sensitivity of decisions increase. If an activity is conducted without appropriate segregation of duties, management should require an independent review (e.g., audit) of that activity.	Functional	Intersects With	Auditing Use of Privileged Functions	IAC-30.4	Mechanisms exist to audit the execution of privileged functions.	3		IAC-21.4

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.7.c	N/A	Segregation of Duties Segregation of duties, or job designs that require more than one person to complete critical or sensitive tasks, can help mitigate risk. Employees and third parties with access to sensitive resources could cause substantial damage and potential loss. System administrators, for instance, have the most powerful role in the user access process and have unlimited access to an institution's information assets and technology. Given this extensive access, management should evaluate the process for determining which individuals should be granted system administrator privileges. Such access should be appropriately monitored for unauthorized or inappropriate activity. Management should incorporate independent reviews or approvals for individuals who perform multiple functions to minimize the potential for fraud, irregularities, and errors. Examples of segregation of duties include the following: • Independent monitoring of the activities performed by the users with increased privileges (e.g., system administrators and super users23). • Distribution of system administration activities so no administrator can hide his or her activities or control an entire system. • Additional levels of approval as the criticality and sensitivity of decisions increase. If an activity is conducted without appropriate segregation of duties, management should require an independent review (e.g., audit) of that activity.	Functional	Intersects With	Privileged User Oversight	MON-14.2	Mechanisms exist to implement enhanced activity monitoring for privileged users.	5		MON-01.15
II.C.7.d	N/A	Confidentiality Agreements The institution should protect the confidentiality of customer and institution information. A breach in confidentiality could disclose proprietary information, increase fraud risk, violate customer privacy and associated rights, and violate laws or regulations. Confidentiality agreements can be used to put all parties on notice that the financial institution owns its information, expects strict confidentiality, and prohibits information sharing outside of that required for legitimate business needs. Management should obtain signed confidentiality agreements before granting employees and contractors access to IT systems.	Functional	Intersects With	Access Agreements	HRS-07	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5		HRS-06
II.C.7.d	N/A	Confidentiality Agreements The institution should protect the confidentiality of customer and institution information. A breach in confidentiality could disclose proprietary information, increase fraud risk, violate customer privacy and associated rights, and violate laws or regulations. Confidentiality agreements can be used to put all parties on notice that the financial institution owns its information, expects strict confidentiality, and prohibits information sharing outside of that required for legitimate business needs. Management should obtain signed confidentiality agreements before granting employees and contractors access to IT systems.	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	8		HRS-06.1
II.C.7.e	N/A	Training Training ensures personnel have the necessary knowledge and skills to perform their job functions.24 Training should support security awareness and strengthen compliance with security and acceptable use policies. Ultimately, management's behavior and priorities heavily influence employee awareness and policy compliance, so training and the commitment to security should start with management. Management should educate users about their security roles and responsibilities and communicate them through acceptable use policies. Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected. Management should have the ability to impose sanctions for noncompliance. Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. The institution should collect signed acknowledgments of the employee acceptable use policy as part of the annual training program. 23 In computing, the super user is a special user account used for system administration. Depending on the operating system, the name of this account might be root, administrator, admin, or supervisor. 24 See also Information Security Standards, section III.C.2, requiring each financial institution to train staff to implement its information security program.	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
II.C.7.e	N/A	Training Training ensures personnel have the necessary knowledge and skills to perform their job functions.24 Training should support security awareness and strengthen compliance with security and acceptable use policies. Ultimately, management's behavior and priorities heavily influence employee awareness and policy compliance, so training and the commitment to security should start with management. Management should educate users about their security roles and responsibilities and communicate them through acceptable use policies. Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected. Management should have the ability to impose sanctions for noncompliance. Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. The institution should collect signed acknowledgments of the employee acceptable use policy as part of the annual training program. 23 In computing, the super user is a special user account used for system administration. Depending on the operating system, the name of this account might be root, administrator, admin, or supervisor. 24 See also Information Security Standards, section III.C.2, requiring each financial institution to train staff to implement its information security program.	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-08.2	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	5		HRS-05.7

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.7.e	N/A	Training Training ensures personnel have the necessary knowledge and skills to perform their job functions.24 Training should support security awareness and strengthen compliance with security and acceptable use policies. Ultimately, management's behavior and priorities heavily influence employee awareness and policy compliance, so training and the commitment to security should start with management. Management should educate users about their security roles and responsibilities and communicate them through acceptable use policies. Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected. Management should have the ability to impose sanctions for noncompliance. Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. The institution should collect signed acknowledgments of the employee acceptable use policy as part of the annual training program. 23 In computing, the super user is a special user account used for system administration. Depending on the operating system, the name of this account might be root, administrator, admin, or supervisor. 24 See also Information Security Standards, section III.C.2, requiring each financial institution to train staff to implement its information security program.	Functional	Intersects With	Personnel Sanctions	HRS-10	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5		HRS-07
II.C.7.e	N/A	Training Training ensures personnel have the necessary knowledge and skills to perform their job functions.24 Training should support security awareness and strengthen compliance with security and acceptable use policies. Ultimately, management's behavior and priorities heavily influence employee awareness and policy compliance, so training and the commitment to security should start with management. Management should educate users about their security roles and responsibilities and communicate them through acceptable use policies. Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected. Management should have the ability to impose sanctions for noncompliance. Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. The institution should collect signed acknowledgments of the employee acceptable use policy as part of the annual training program. 23 In computing, the super user is a special user account used for system administration. Depending on the operating system, the name of this account might be root, administrator, admin, or supervisor. 24 See also Information Security Standards, section III.C.2, requiring each financial institution to train staff to implement its information security program.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8		SAT-02
II.C.7.e	N/A	Training Training ensures personnel have the necessary knowledge and skills to perform their job functions.24 Training should support security awareness and strengthen compliance with security and acceptable use policies. Ultimately, management's behavior and priorities heavily influence employee awareness and policy compliance, so training and the commitment to security should start with management. Management should educate users about their security roles and responsibilities and communicate them through acceptable use policies. Management should hold all employees, officers, and contractors accountable for complying with security and acceptable use policies and should ensure that the institution's information and other assets are protected. Management should have the ability to impose sanctions for noncompliance. Training materials for most users focus on issues such as end-point security, log-in requirements, and password administration guidelines. Training programs should include scenarios capturing areas of significant and growing concern, such as phishing and social engineering attempts, loss of data through e-mail or removable media, or unintentional posting of confidential or proprietary information on social media. As the risk environment changes, so should the training. The institution should collect signed acknowledgments of the employee acceptable use policy as part of the annual training program. 23 In computing, the super user is a special user account used for system administration. Depending on the operating system, the name of this account might be root, administrator, admin, or supervisor. 24 See also Information Security Standards, section III.C.2, requiring each financial institution to train staff to implement its information security program.	Functional	Intersects With	Social Engineering & Mining	SAT-06.1	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5		SAT-02.2
II.C.8	N/A	Physical Security Action Summary Management should implement appropriate preventive, detective, and corrective controls for physical security. Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information. Management should implement appropriate preventive, detective, and corrective controls for mitigating the risks inherent to those physical security zones. A data center houses an institution's most important information system components. When selecting a site for a data center, one major objective should be to limit the risk of exposure from internal and external threats, including, where possible, environmental threats inherent to physical locations (e.g., hurricanes, earthquakes, and blizzards). The selection process should include reviewing the surrounding area to determine whether it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Guards, fences, barriers, surveillance equipment, or other devices can deter intruders. Because access to key information systems' hardware and software should be limited, appropriate physical controls should be in place. Additionally, the location should not be identified or advertised by signage or other indicators. Detection devices, when applicable, should be used to prevent theft and safeguard the equipment. The devices should provide continuous coverage. Detection devices have two purposes-to send alarms when responses are necessary and to support subsequent forensics. Alarms are useful only when response will occur. Some detection devices include the following: • Switches that activate alarms when electrical circuits are broken. • Light and laser beams, ultraviolet beams, sound, or vibration detectors that are invisible to intruders, and ultrasonic or radar devices that detect movement. • Closed-circuit television (CCTV) that provides visual observation and records intrusions. A combination of fire suppression, smoke alarms, raised flooring, and heat and	Functional	Intersects With	Removal of Assets	AST-24	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	5		AST-11

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.8	N/A	Physical Security Action Summary Management should implement appropriate preventive, detective, and corrective controls for physical security. Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information. Management should implement appropriate preventive, detective, and corrective controls for mitigating the risks inherent to those physical security zones. A data center houses an institution's most important information system components. When selecting a site for a data center, one major objective should be to limit the risk of exposure from internal and external threats, including, where possible, environmental threats inherent to physical locations (e.g., hurricanes, earthquakes, and blizzards). The selection process should include reviewing the surrounding area to determine whether it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Guards, fences, barriers, surveillance equipment, or other devices can deter intruders. Because access to key information systems' hardware and software should be limited, appropriate physical controls should be in place. Additionally, the location should not be identified or advertised by signage or other indicators. Detection devices, when applicable, should be used to prevent theft and safeguard the equipment. The devices should provide continuous coverage. Detection devices have two purposes-to send alarms when responses are necessary and to support subsequent forensics. Alarms are useful only when response will occur. Some detection devices include the following: • Switches that activate alarms when electrical circuits are broken. • Light and laser beams, ultraviolet beams, sound, or vibration detectors that are invisible to intruders, and ultrasonic or radar devices that detect movement. • Closed-circuit television (CCTV) that provides visual observation and records intrusions. A combination of fire suppression, smoke alarms, raised flooring, and heat and	Functional	Intersects With	Physical & Environmental Protections	PES-02	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5		PES-01
II.C.8	N/A	Physical Security Action Summary Management should implement appropriate preventive, detective, and corrective controls for physical security. Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information. Management should implement appropriate preventive, detective, and corrective controls for mitigating the risks inherent to those physical security zones. A data center houses an institution's most important information system components. When selecting a site for a data center, one major objective should be to limit the risk of exposure from internal and external threats, including, where possible, environmental threats inherent to physical locations (e.g., hurricanes, earthquakes, and blizzards). The selection process should include reviewing the surrounding area to determine whether it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Guards, fences, barriers, surveillance equipment, or other devices can deter intruders. Because access to key information systems' hardware and software should be limited, appropriate physical controls should be in place. Additionally, the location should not be identified or advertised by signage or other indicators. Detection devices, when applicable, should be used to prevent theft and safeguard the equipment. The devices should provide continuous coverage. Detection devices have two purposes-to send alarms when responses are necessary and to support subsequent forensics. Alarms are useful only when response will occur. Some detection devices include the following: • Switches that activate alarms when electrical circuits are broken. • Light and laser beams, ultraviolet beams, sound, or vibration detectors that are invisible to intruders, and ultrasonic or radar devices that detect movement. • Closed-circuit television (CCTV) that provides visual observation and records intrusions. A combination of fire suppression, smoke alarms, raised flooring, and heat and	Functional	Intersects With	Physical Access Control	PES-08	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5		PES-03
II.C.8	N/A	Physical Security Action Summary Management should implement appropriate preventive, detective, and corrective controls for physical security. Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information. Management should implement appropriate preventive, detective, and corrective controls for mitigating the risks inherent to those physical security zones. A data center houses an institution's most important information system components. When selecting a site for a data center, one major objective should be to limit the risk of exposure from internal and external threats, including, where possible, environmental threats inherent to physical locations (e.g., hurricanes, earthquakes, and blizzards). The selection process should include reviewing the surrounding area to determine whether it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Guards, fences, barriers, surveillance equipment, or other devices can deter intruders. Because access to key information systems' hardware and software should be limited, appropriate physical controls should be in place. Additionally, the location should not be identified or advertised by signage or other indicators. Detection devices, when applicable, should be used to prevent theft and safeguard the equipment. The devices should provide continuous coverage. Detection devices have two purposes-to send alarms when responses are necessary and to support subsequent forensics. Alarms are useful only when response will occur. Some detection devices include the following: • Switches that activate alarms when electrical circuits are broken. • Light and laser beams, ultraviolet beams, sound, or vibration detectors that are invisible to intruders, and ultrasonic or radar devices that detect movement. • Closed-circuit television (CCTV) that provides visual observation and records intrusions. A combination of fire suppression, smoke alarms, raised flooring, and heat and	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-13.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5		PES-05.1

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL:	https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL:	https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.8	N/A	Physical Security Action Summary Management should implement appropriate preventive, detective, and corrective controls for physical security. Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information. Management should implement appropriate preventive, detective, and corrective controls for mitigating the risks inherent to those physical security zones. A data center houses an institution's most important information system components. When selecting a site for a data center, one major objective should be to limit the risk of exposure from internal and external threats, including, where possible, environmental threats inherent to physical locations (e.g., hurricanes, earthquakes, and blizzards). The selection process should include reviewing the surrounding area to determine whether it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Guards, fences, barriers, surveillance equipment, or other devices can deter intruders. Because access to key information systems' hardware and software should be limited, appropriate physical controls should be in place. Additionally, the location should not be identified or advertised by signage or other indicators. Detection devices, when applicable, should be used to prevent theft and safeguard the equipment. The devices should provide continuous coverage. Detection devices have two purposes-to send alarms when responses are necessary and to support subsequent forensics. Alarms are useful only when response will occur. Some detection devices include the following: • Switches that activate alarms when electrical circuits are broken. • Light and laser beams, ultraviolet beams, sound, or vibration detectors that are invisible to intruders, and ultrasonic or radar devices that detect movement. • Closed-circuit television (CCTV) that provides visual observation and records intrusions. A combination of fire suppression, smoke alarms, raised flooring, and heat and	Functional	Intersects With	Equipment Siting & Protection	PES-16	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5		PES-12
II.C.8	N/A	Physical Security Action Summary Management should implement appropriate preventive, detective, and corrective controls for physical security. Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information. Management should implement appropriate preventive, detective, and corrective controls for mitigating the risks inherent to those physical security zones. A data center houses an institution's most important information system components. When selecting a site for a data center, one major objective should be to limit the risk of exposure from internal and external threats, including, where possible, environmental threats inherent to physical locations (e.g., hurricanes, earthquakes, and blizzards). The selection process should include reviewing the surrounding area to determine whether it is relatively safe from exposure to fire, flood, explosion, or similar environmental hazards. Guards, fences, barriers, surveillance equipment, or other devices can deter intruders. Because access to key information systems' hardware and software should be limited, appropriate physical controls should be in place. Additionally, the location should not be identified or advertised by signage or other indicators. Detection devices, when applicable, should be used to prevent theft and safeguard the equipment. The devices should provide continuous coverage. Detection devices have two purposes-to send alarms when responses are necessary and to support subsequent forensics. Alarms are useful only when response will occur. Some detection devices include the following: • Switches that activate alarms when electrical circuits are broken. • Light and laser beams, ultraviolet beams, sound, or vibration detectors that are invisible to intruders, and ultrasonic or radar devices that detect movement. • Closed-circuit television (CCTV) that provides visual observation and records intrusions. A combination of fire suppression, smoke alarms, raised flooring, and heat and	Functional	Intersects With	Fire Protection	PES-26	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	5		PES-08
II.C.9	Threat Intelligence and Information Sharing	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.C.9.a	N/A	Wireless Network Considerations A wireless LAN (WLAN) is a medium of network connectivity, supported by radio wave transmissions that provides more convenient network access to employees or devices that need flexibility to connect to multiple locations within the institution's facilities. Because the user is not physically connected to the network and the wireless signal is broadcast and available to others, wireless networks are inherently less secure than wired networks and require additional scrutiny, controls, and oversight. Wireless access points are the devices that broadcast the radio wave signals and should be physically secure to prevent compromise and securely configured to provide the same level of control as a wired connection. Wireless gateways can allow management to implement more complex access controls, including advanced identity management capabilities and services to detect and remediate malicious software. Policies should prohibit installation of wireless access points and gateways without approval and formal inclusion in the hardware inventory. Network monitoring systems should be configured to detect the addition of new devices. Alternatively, network access control (NAC) systems could prevent the recognition of any unauthorized device.27 Management should consider limiting the WLAN signal to authorized areas, within the boundaries of the institution, if feasible. Management should use an industry-accepted level of encryption with strength commensurate with the institution's risk profile on the institution's wireless networks. Malicious insiders and attackers may also set up rogue or unauthorized wireless access points and trick employees into connecting. Such access points allow attackers to monitor employee activities. The institution should scan the network regularly to detect rogue access points and consider implementing NAC systems to prevent the successful connection of unauthorized devices. 26 VOIP is the transmission of voice telephone conversations using the Internet or IP	Functional	Intersects With	Wireless Access Authentication & Encryption	CFG-04.8	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	5		CRY-07

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL:	https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL:	https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.9.a	N/A	Wireless Network Considerations A wireless LAN (WLAN) is a medium of network connectivity, supported by radio wave transmissions that provides more convenient network access to employees or devices that need flexibility to connect to multiple locations within the institution's facilities. Because the user is not physically connected to the network and the wireless signal is broadcast and available to others, wireless networks are inherently less secure than wired networks and require additional scrutiny, controls, and oversight. Wireless access points are the devices that broadcast the radio wave signals and should be physically secure to prevent compromise and securely configured to provide the same level of control as a wired connection. Wireless gateways can allow management to implement more complex access controls, including advanced identity management capabilities and services to detect and remediate malicious software. Policies should prohibit installation of wireless access points and gateways without approval and formal inclusion in the hardware inventory. Network monitoring systems should be configured to detect the addition of new devices. Alternatively, network access control (NAC) systems could prevent the recognition of any unauthorized device.27 Management should consider limiting the WLAN signal to authorized areas, within the boundaries of the institution, if feasible. Management should use an industry-accepted level of encryption with strength commensurate with the institution's risk profile on the institution's wireless networks. Malicious insiders and attackers may also set up rogue or unauthorized wireless access points and trick employees into connecting. Such access points allow attackers to monitor employee activities. The institution should scan the network regularly to detect rogue access points and consider implementing NAC systems to prevent the successful connection of unauthorized devices. 26 VOIP is the transmission of voice telephone conversations using the Internet or IP	Functional	Intersects With	Network Access Control (NAC)	NET-16	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	3		AST-02.5
II.C.9.a	N/A	Wireless Network Considerations A wireless LAN (WLAN) is a medium of network connectivity, supported by radio wave transmissions that provides more convenient network access to employees or devices that need flexibility to connect to multiple locations within the institution's facilities. Because the user is not physically connected to the network and the wireless signal is broadcast and available to others, wireless networks are inherently less secure than wired networks and require additional scrutiny, controls, and oversight. Wireless access points are the devices that broadcast the radio wave signals and should be physically secure to prevent compromise and securely configured to provide the same level of control as a wired connection. Wireless gateways can allow management to implement more complex access controls, including advanced identity management capabilities and services to detect and remediate malicious software. Policies should prohibit installation of wireless access points and gateways without approval and formal inclusion in the hardware inventory. Network monitoring systems should be configured to detect the addition of new devices. Alternatively, network access control (NAC) systems could prevent the recognition of any unauthorized device.27 Management should consider limiting the WLAN signal to authorized areas, within the boundaries of the institution, if feasible. Management should use an industry-accepted level of encryption with strength commensurate with the institution's risk profile on the institution's wireless networks. Malicious insiders and attackers may also set up rogue or unauthorized wireless access points and trick employees into connecting. Such access points allow attackers to monitor employee activities. The institution should scan the network regularly to detect rogue access points and consider implementing NAC systems to prevent the successful connection of unauthorized devices. 26 VOIP is the transmission of voice telephone conversations using the Internet or IP	Functional	Intersects With	Guest Networks	NET-22	Mechanisms exist to implement and manage a secure guest network.	5		NET-02.2
II.C.9.a	N/A	Wireless Network Considerations A wireless LAN (WLAN) is a medium of network connectivity, supported by radio wave transmissions that provides more convenient network access to employees or devices that need flexibility to connect to multiple locations within the institution's facilities. Because the user is not physically connected to the network and the wireless signal is broadcast and available to others, wireless networks are inherently less secure than wired networks and require additional scrutiny, controls, and oversight. Wireless access points are the devices that broadcast the radio wave signals and should be physically secure to prevent compromise and securely configured to provide the same level of control as a wired connection. Wireless gateways can allow management to implement more complex access controls, including advanced identity management capabilities and services to detect and remediate malicious software. Policies should prohibit installation of wireless access points and gateways without approval and formal inclusion in the hardware inventory. Network monitoring systems should be configured to detect the addition of new devices. Alternatively, network access control (NAC) systems could prevent the recognition of any unauthorized device.27 Management should consider limiting the WLAN signal to authorized areas, within the boundaries of the institution, if feasible. Management should use an industry-accepted level of encryption with strength commensurate with the institution's risk profile on the institution's wireless networks. Malicious insiders and attackers may also set up rogue or unauthorized wireless access points and trick employees into connecting. Such access points allow attackers to monitor employee activities. The institution should scan the network regularly to detect rogue access points and consider implementing NAC systems to prevent the successful connection of unauthorized devices. 26 VOIP is the transmission of voice telephone conversations using the Internet or IP	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	8		NET-15

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.9.a	N/A	Wireless Network Considerations A wireless LAN (WLAN) is a medium of network connectivity, supported by radio wave transmissions that provides more convenient network access to employees or devices that need flexibility to connect to multiple locations within the institution's facilities. Because the user is not physically connected to the network and the wireless signal is broadcast and available to others, wireless networks are inherently less secure than wired networks and require additional scrutiny, controls, and oversight. Wireless access points are the devices that broadcast the radio wave signals and should be physically secure to prevent compromise and securely configured to provide the same level of control as a wired connection. Wireless gateways can allow management to implement more complex access controls, including advanced identity management capabilities and services to detect and remediate malicious software. Policies should prohibit installation of wireless access points and gateways without approval and formal inclusion in the hardware inventory. Network monitoring systems should be configured to detect the addition of new devices. Alternatively, network access control (NAC) systems could prevent the recognition of any unauthorized device.27 Management should consider limiting the WLAN signal to authorized areas, within the boundaries of the institution, if feasible. Management should use an industry-accepted level of encryption with strength commensurate with the institution's risk profile on the institution's wireless networks. Malicious insiders and attackers may also set up rogue or unauthorized wireless access points and trick employees into connecting. Such access points allow attackers to monitor employee activities. The institution should scan the network regularly to detect rogue access points and consider implementing NAC systems to prevent the successful connection of unauthorized devices. 26 VOIP is the transmission of voice telephone conversations using the Internet or IP	Functional	Intersects With	Rogue Wireless Detection	NET-25	Mechanisms exist to test for the presence of Wireless Access Points (WAPs) and identify all authorized and unauthorized WAPs within the facility(ies).	5		NET-15.5
II.C.9.a	N/A	Wireless Network Considerations A wireless LAN (WLAN) is a medium of network connectivity, supported by radio wave transmissions that provides more convenient network access to employees or devices that need flexibility to connect to multiple locations within the institution's facilities. Because the user is not physically connected to the network and the wireless signal is broadcast and available to others, wireless networks are inherently less secure than wired networks and require additional scrutiny, controls, and oversight. Wireless access points are the devices that broadcast the radio wave signals and should be physically secure to prevent compromise and securely configured to provide the same level of control as a wired connection. Wireless gateways can allow management to implement more complex access controls, including advanced identity management capabilities and services to detect and remediate malicious software. Policies should prohibit installation of wireless access points and gateways without approval and formal inclusion in the hardware inventory. Network monitoring systems should be configured to detect the addition of new devices. Alternatively, network access control (NAC) systems could prevent the recognition of any unauthorized device.27 Management should consider limiting the WLAN signal to authorized areas, within the boundaries of the institution, if feasible. Management should use an industry-accepted level of encryption with strength commensurate with the institution's risk profile on the institution's wireless networks. Malicious insiders and attackers may also set up rogue or unauthorized wireless access points and trick employees into connecting. Such access points allow attackers to monitor employee activities. The institution should scan the network regularly to detect rogue access points and consider implementing NAC systems to prevent the successful connection of unauthorized devices. 26 VOIP is the transmission of voice telephone conversations using the Internet or IP	Functional	Intersects With	Remote Access Cryptographic Protections	NET-26.5	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	5		NET-14.2
II.C.10	Configuration Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.C.10.a	N/A	Configuration management is a process to securely maintain the institution's technology by developing expected baselines for tracking, controlling, and managing systems settings. To mitigate information security risk, management should control configurations of systems, applications, and other technology. Effective configuration management relies on policies and procedures to ensure compliance with minimally acceptable system configuration requirements. When information systems change, management should update baselines; confirm security settings; and track, verify, and report configuration items. Configurations should be monitored for unauthorized changes, and misconfigurations should be identified. Management can use automated solutions to help track, manage, and identify necessary corrections.	Functional	Intersects With	Configuration Management Program	CFG-02	Mechanisms exist to facilitate the implementation of configuration management controls.	5		CFG-01
II.C.10.a	N/A	Configuration management is a process to securely maintain the institution's technology by developing expected baselines for tracking, controlling, and managing systems settings. To mitigate information security risk, management should control configurations of systems, applications, and other technology. Effective configuration management relies on policies and procedures to ensure compliance with minimally acceptable system configuration requirements. When information systems change, management should update baselines; confirm security settings; and track, verify, and report configuration items. Configurations should be monitored for unauthorized changes, and misconfigurations should be identified. Management can use automated solutions to help track, manage, and identify necessary corrections.	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
II.C.10.a	N/A	Configuration management is a process to securely maintain the institution's technology by developing expected baselines for tracking, controlling, and managing systems settings. To mitigate information security risk, management should control configurations of systems, applications, and other technology. Effective configuration management relies on policies and procedures to ensure compliance with minimally acceptable system configuration requirements. When information systems change, management should update baselines; confirm security settings; and track, verify, and report configuration items. Configurations should be monitored for unauthorized changes, and misconfigurations should be identified. Management can use automated solutions to help track, manage, and identify necessary corrections.	Functional	Intersects With	Baseline Configuration Reviews & Updates	CFG-07	Mechanisms exist to review and update secure baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5		CFG-02.1
II.C.10.a	N/A	Configuration management is a process to securely maintain the institution's technology by developing expected baselines for tracking, controlling, and managing systems settings. To mitigate information security risk, management should control configurations of systems, applications, and other technology. Effective configuration management relies on policies and procedures to ensure compliance with minimally acceptable system configuration requirements. When information systems change, management should update baselines; confirm security settings; and track, verify, and report configuration items. Configurations should be monitored for unauthorized changes, and misconfigurations should be identified. Management can use automated solutions to help track, manage, and identify necessary corrections.	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	5		CFG-06

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL:	https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL:	https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.10.b	N/A	Institutions typically use commercial off-the-shelf (COTS) software for operating systems and applications, on such diverse platforms as network infrastructure, servers, desktops, laptops, and mobile devices. COTS systems generally provide more functions than are required for the specific purposes for which they are employed. A default installation of a server operating system may include mail, web, and file-sharing services on a system that does not require those functions. Unnecessary software and services represent a potential security weakness. Their presence increases the potential number of discovered and undiscovered vulnerabilities in the system. Additionally, system administrators may not install patches or monitor the unused software and services to the same degree as they would operational software and services. Protection against those risks begins when the systems are constructed and software installed through a process that is referred to as hardening a system. Management should consult operating system and software vendor-recommended security controls. When deploying COTS applications and systems, management should harden the resulting applications and systems. Hardening can include the following actions: • Determining the purpose of the applications and systems and documenting minimum software and hardware requirements and services to be included. • Installing the minimum hardware, software, and services necessary to meet the requirements using a documented installation procedure. • Installing necessary patches. • Installing the most secure and up-to-date versions of applications. • Configuring privilege and access controls by first denying all, then granting back the minimum necessary to each user (i.e., enforcing the principle of least privilege). • Configuring security settings as appropriate, enabling allowed activity, and prohibiting non- approved activities. • Enabling logging. • Creating cryptographic hashes31 of key files. • Archiving the	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03
II.C.10.b	N/A	Institutions typically use commercial off-the-shelf (COTS) software for operating systems and applications, on such diverse platforms as network infrastructure, servers, desktops, laptops, and mobile devices. COTS systems generally provide more functions than are required for the specific purposes for which they are employed. A default installation of a server operating system may include mail, web, and file-sharing services on a system that does not require those functions. Unnecessary software and services represent a potential security weakness. Their presence increases the potential number of discovered and undiscovered vulnerabilities in the system. Additionally, system administrators may not install patches or monitor the unused software and services to the same degree as they would operational software and services. Protection against those risks begins when the systems are constructed and software installed through a process that is referred to as hardening a system. Management should consult operating system and software vendor-recommended security controls. When deploying COTS applications and systems, management should harden the resulting applications and systems. Hardening can include the following actions: • Determining the purpose of the applications and systems and documenting minimum software and hardware requirements and services to be included. • Installing the minimum hardware, software, and services necessary to meet the requirements using a documented installation procedure. • Installing necessary patches. • Installing the most secure and up-to-date versions of applications. • Configuring privilege and access controls by first denying all, then granting back the minimum necessary to each user (i.e., enforcing the principle of least privilege). • Configuring security settings as appropriate, enabling allowed activity, and prohibiting non- approved activities. • Enabling logging. • Creating cryptographic hashes31 of key files. • Archiving the	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
II.C.10.b	N/A	Institutions typically use commercial off-the-shelf (COTS) software for operating systems and applications, on such diverse platforms as network infrastructure, servers, desktops, laptops, and mobile devices. COTS systems generally provide more functions than are required for the specific purposes for which they are employed. A default installation of a server operating system may include mail, web, and file-sharing services on a system that does not require those functions. Unnecessary software and services represent a potential security weakness. Their presence increases the potential number of discovered and undiscovered vulnerabilities in the system. Additionally, system administrators may not install patches or monitor the unused software and services to the same degree as they would operational software and services. Protection against those risks begins when the systems are constructed and software installed through a process that is referred to as hardening a system. Management should consult operating system and software vendor-recommended security controls. When deploying COTS applications and systems, management should harden the resulting applications and systems. Hardening can include the following actions: • Determining the purpose of the applications and systems and documenting minimum software and hardware requirements and services to be included. • Installing the minimum hardware, software, and services necessary to meet the requirements using a documented installation procedure. • Installing necessary patches. • Installing the most secure and up-to-date versions of applications. • Configuring privilege and access controls by first denying all, then granting back the minimum necessary to each user (i.e., enforcing the principle of least privilege). • Configuring security settings as appropriate, enabling allowed activity, and prohibiting non- approved activities. • Enabling logging. • Creating cryptographic hashes31 of key files. • Archiving the	Functional	Intersects With	Default Authenticators	IAC-14.4	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5		IAC-10.8
II.C.10.c	N/A	Standard Builds Consistency in system configuration makes security easier to implement and maintain. The institution should use standard builds, which allow one documented configuration to be applied to multiple computers in a controlled manner. Some institutions, depending on their size and complexity, may have many standard builds for the different system configurations needed to address various business functions. Through standard builds, an institution simplifies the following activities: • Creating hardware and software inventories. • Updating and patching systems. • Restoring systems in the event of a disaster or outage. • Investigating anomalous activity. • Auditing configurations for conformance with the approved configuration. The institution may not be able to meet all of its requirements from its standard builds. The use of nonstandard builds should be documented and approved by management, with appropriate changes made to patch management and disaster recovery plans. 31 A hash is a fixed-length cryptographic output of variables, such as a message, being operated on by a formula or cryptographic algorithm. 32 A checksum is a simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message, which allows the receiver to verify the accuracy of the message.	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

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.10.c	N/A	Standard Builds Consistency in system configuration makes security easier to implement and maintain. The institution should use standard builds, which allow one documented configuration to be applied to multiple computers in a controlled manner. Some institutions, depending on their size and complexity, may have many standard builds for the different system configurations needed to address various business functions. Through standard builds, an institution simplifies the following activities: • Creating hardware and software inventories. • Updating and patching systems. • Restoring systems in the event of a disaster or outage. • Investigating anomalous activity. • Auditing configurations for conformance with the approved configuration. The institution may not be able to meet all of its requirements from its standard builds. The use of nonstandard builds should be documented and approved by management, with appropriate changes made to patch management and disaster recovery plans. 31 A hash is a fixed-length cryptographic output of variables, such as a message, being operated on by a formula or cryptographic algorithm. 32 A checksum is a simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message, which allows the receiver to verify the accuracy of the message.	Functional	Intersects With	Approved Configuration Deviations	CFG-06	Mechanisms exist to document, assess and approve or deny deviations to secure baseline configurations.	5		CFG-02.7
II.C.10.d	N/A	Frequently, security vulnerabilities are discovered in operating systems and other software after deployment. Hackers often will attempt to exploit these known vulnerabilities to try to gain access to the institution's systems. Third parties issue patches to address vulnerabilities found on institution systems and applications.33 Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated. In addition, management should use vulnerability scanners periodically to identify vulnerabilities in a timely manner. As part of the institution's patch management process, management should establish and implement the following: • A monitoring process that identifies the availability of software patches. • A process to evaluate the patches against the threat and network environment. • A prioritization process to determine which patches to apply across classes of computers and applications. • A process for obtaining, testing, and securely installing patches, including in the institution's virtual environments. • An exception process, with appropriate documentation, for patches that management decides to delay or not apply. • A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment in a timely manner. • A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied. The institution should have procedures that include how to implement patches to mitigate risks of changing systems and address systems with unique configurations. Before applying a patch, management should back up the production system. Additionally, management should define appropriate patch windows and, whenever possible, restrict the implementation of patches to defined time	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
II.C.10.d	N/A	Frequently, security vulnerabilities are discovered in operating systems and other software after deployment. Hackers often will attempt to exploit these known vulnerabilities to try to gain access to the institution's systems. Third parties issue patches to address vulnerabilities found on institution systems and applications.33 Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated. In addition, management should use vulnerability scanners periodically to identify vulnerabilities in a timely manner. As part of the institution's patch management process, management should establish and implement the following: • A monitoring process that identifies the availability of software patches. • A process to evaluate the patches against the threat and network environment. • A prioritization process to determine which patches to apply across classes of computers and applications. • A process for obtaining, testing, and securely installing patches, including in the institution's virtual environments. • An exception process, with appropriate documentation, for patches that management decides to delay or not apply. • A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment in a timely manner. • A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied. The institution should have procedures that include how to implement patches to mitigate risks of changing systems and address systems with unique configurations. Before applying a patch, management should back up the production system. Additionally, management should define appropriate patch windows and, whenever possible, restrict the implementation of patches to defined time	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8		VPM-05
II.C.10.d	N/A	Frequently, security vulnerabilities are discovered in operating systems and other software after deployment. Hackers often will attempt to exploit these known vulnerabilities to try to gain access to the institution's systems. Third parties issue patches to address vulnerabilities found on institution systems and applications.33 Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated. In addition, management should use vulnerability scanners periodically to identify vulnerabilities in a timely manner. As part of the institution's patch management process, management should establish and implement the following: • A monitoring process that identifies the availability of software patches. • A process to evaluate the patches against the threat and network environment. • A prioritization process to determine which patches to apply across classes of computers and applications. • A process for obtaining, testing, and securely installing patches, including in the institution's virtual environments. • An exception process, with appropriate documentation, for patches that management decides to delay or not apply. • A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment in a timely manner. • A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied. The institution should have procedures that include how to implement patches to mitigate risks of changing systems and address systems with unique configurations. Before applying a patch, management should back up the production system. Additionally, management should define appropriate patch windows and, whenever possible, restrict the implementation of patches to defined time	Functional	Intersects With	Software Patch Integrity	VPM-08.2	Mechanisms exist to ensure software and/or firmware patches are: (1) Obtained from trusted sources; and (2) Checked for integrity.	5		VPM-05.8

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.10.d	N/A	Frequently, security vulnerabilities are discovered in operating systems and other software after deployment. Hackers often will attempt to exploit these known vulnerabilities to try to gain access to the institution's systems. Third parties issue patches to address vulnerabilities found on institution systems and applications.33 Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated. In addition, management should use vulnerability scanners periodically to identify vulnerabilities in a timely manner. As part of the institution's patch management process, management should establish and implement the following: • A monitoring process that identifies the availability of software patches. • A process to evaluate the patches against the threat and network environment. • A prioritization process to determine which patches to apply across classes of computers and applications. • A process for obtaining, testing, and securely installing patches, including in the institution's virtual environments. • An exception process, with appropriate documentation, for patches that management decides to delay or not apply. • A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment in a timely manner. • A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied. The institution should have procedures that include how to implement patches to mitigate risks of changing systems and address systems with unique configurations. Before applying a patch, management should back up the production system. Additionally, management should define appropriate patch windows and, whenever possible, restrict the implementation of patches to defined time	Functional	Intersects With	Deferred Patching Decisions	VPM-09	Mechanisms exist to facilitate the deferral of software and/or firmware patches when the disadvantages of applying the patch outweigh the benefits.	5		VPM-04.3
II.C.10.d	N/A	Frequently, security vulnerabilities are discovered in operating systems and other software after deployment. Hackers often will attempt to exploit these known vulnerabilities to try to gain access to the institution's systems. Third parties issue patches to address vulnerabilities found on institution systems and applications.33 Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated. In addition, management should use vulnerability scanners periodically to identify vulnerabilities in a timely manner. As part of the institution's patch management process, management should establish and implement the following: • A monitoring process that identifies the availability of software patches. • A process to evaluate the patches against the threat and network environment. • A prioritization process to determine which patches to apply across classes of computers and applications. • A process for obtaining, testing, and securely installing patches, including in the institution's virtual environments. • An exception process, with appropriate documentation, for patches that management decides to delay or not apply. • A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment in a timely manner. • A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied. The institution should have procedures that include how to implement patches to mitigate risks of changing systems and address systems with unique configurations. Before applying a patch, management should back up the production system. Additionally, management should define appropriate patch windows and, whenever possible, restrict the implementation of patches to defined time	Functional	Intersects With	Pre-Deployment Patch Testing	VPM-10	Mechanisms exist to perform due diligence on software and/or firmware update stability by conducting pre-production testing in a non-production environment.	5		VPM-05.6
II.C.10.d	N/A	Frequently, security vulnerabilities are discovered in operating systems and other software after deployment. Hackers often will attempt to exploit these known vulnerabilities to try to gain access to the institution's systems. Third parties issue patches to address vulnerabilities found on institution systems and applications.33 Management should implement automated patch management systems and software to ensure all network components (virtual machines, routers, switches, mobile devices, firewalls, etc.) are appropriately updated. In addition, management should use vulnerability scanners periodically to identify vulnerabilities in a timely manner. As part of the institution's patch management process, management should establish and implement the following: • A monitoring process that identifies the availability of software patches. • A process to evaluate the patches against the threat and network environment. • A prioritization process to determine which patches to apply across classes of computers and applications. • A process for obtaining, testing, and securely installing patches, including in the institution's virtual environments. • An exception process, with appropriate documentation, for patches that management decides to delay or not apply. • A process to ensure that all patches installed in the production environment are also installed in the disaster recovery environment in a timely manner. • A documentation process to ensure the institution's information assets and technology inventory and disaster recovery plans are updated as appropriate when patches are applied. The institution should have procedures that include how to implement patches to mitigate risks of changing systems and address systems with unique configurations. Before applying a patch, management should back up the production system. Additionally, management should define appropriate patch windows and, whenever possible, restrict the implementation of patches to defined time	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.11	N/A	End-of-Life Management Management should plan for a system's life cycle, eventual end of life, and any corresponding security and business impacts. The institution's strategy should incorporate planned changes to systems, including an evaluation of the current environment to identify potential vulnerabilities, upgrade opportunities, or new defense layers. Also included in this strategy should be considerations for the support provided by third-party system vendors and the risks related to operating unsupported legacy systems. Management should have policies to manage both the hardware and software life cycles. Security risks related to reaching a system's end of life include (a) the increased potential for vulnerabilities because the third party no longer provides patches or support, (b) incompatibility with other systems in the institution's environment, and (c) limitations in security features in older or obsolete systems. Effective end-of-life management should include the following: • Maintaining inventories of systems and applications. • Adhering to an approved end-of-life or sunset policy for older systems. • Tracking changes made to the systems and applications, availability of updates, and the planned end of support by the vendor. • Conducting risk assessments on systems and applications to help determine end-of-life. • Planning for the replacement of systems nearing obsolescence and complying with policy requirements for implementing new systems or applications. • Developing specific procedures for the secure destruction or data wiping of hard drives returned to vendors or donated, to prevent the inadvertent disclosure of sensitive information. If an end-of-life system or application must remain in use, management should ensure appropriate mitigating controls are in place, which may include segregating the system or application from the network. Management should also have a plan to replace the system or application and implement compensating	Functional	Intersects With	Technology Lifecycle Management	AST-37	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5		SEA-07.1
II.C.11	N/A	End-of-Life Management Management should plan for a system's life cycle, eventual end of life, and any corresponding security and business impacts. The institution's strategy should incorporate planned changes to systems, including an evaluation of the current environment to identify potential vulnerabilities, upgrade opportunities, or new defense layers. Also included in this strategy should be considerations for the support provided by third-party system vendors and the risks related to operating unsupported legacy systems. Management should have policies to manage both the hardware and software life cycles. Security risks related to reaching a system's end of life include (a) the increased potential for vulnerabilities because the third party no longer provides patches or support, (b) incompatibility with other systems in the institution's environment, and (c) limitations in security features in older or obsolete systems. Effective end-of-life management should include the following: • Maintaining inventories of systems and applications. • Adhering to an approved end-of-life or sunset policy for older systems. • Tracking changes made to the systems and applications, availability of updates, and the planned end of support by the vendor. • Conducting risk assessments on systems and applications to help determine end-of-life. • Planning for the replacement of systems nearing obsolescence and complying with policy requirements for implementing new systems or applications. • Developing specific procedures for the secure destruction or data wiping of hard drives returned to vendors or donated, to prevent the inadvertent disclosure of sensitive information. If an end-of-life system or application must remain in use, management should ensure appropriate mitigating controls are in place, which may include segregating the system or application from the network. Management should also have a plan to replace the system or application and implement compensating	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.	5		TDA-17
II.C.11	N/A	End-of-Life Management Management should plan for a system's life cycle, eventual end of life, and any corresponding security and business impacts. The institution's strategy should incorporate planned changes to systems, including an evaluation of the current environment to identify potential vulnerabilities, upgrade opportunities, or new defense layers. Also included in this strategy should be considerations for the support provided by third-party system vendors and the risks related to operating unsupported legacy systems. Management should have policies to manage both the hardware and software life cycles. Security risks related to reaching a system's end of life include (a) the increased potential for vulnerabilities because the third party no longer provides patches or support, (b) incompatibility with other systems in the institution's environment, and (c) limitations in security features in older or obsolete systems. Effective end-of-life management should include the following: • Maintaining inventories of systems and applications. • Adhering to an approved end-of-life or sunset policy for older systems. • Tracking changes made to the systems and applications, availability of updates, and the planned end of support by the vendor. • Conducting risk assessments on systems and applications to help determine end-of-life. • Planning for the replacement of systems nearing obsolescence and complying with policy requirements for implementing new systems or applications. • Developing specific procedures for the secure destruction or data wiping of hard drives returned to vendors or donated, to prevent the inadvertent disclosure of sensitive information. If an end-of-life system or application must remain in use, management should ensure appropriate mitigating controls are in place, which may include segregating the system or application from the network. Management should also have a plan to replace the system or application and implement compensating	Functional	Intersects With	Alternate Sources for Continued Support	AST-39.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	3		TDA-17.1

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL:	https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL:	https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.11	N/A	End-of-Life Management Management should plan for a system's life cycle, eventual end of life, and any corresponding security and business impacts. The institution's strategy should incorporate planned changes to systems, including an evaluation of the current environment to identify potential vulnerabilities, upgrade opportunities, or new defense layers. Also included in this strategy should be considerations for the support provided by third-party system vendors and the risks related to operating unsupported legacy systems. Management should have policies to manage both the hardware and software life cycles. Security risks related to reaching a system's end of life include (a) the increased potential for vulnerabilities because the third party no longer provides patches or support, (b) incompatibility with other systems in the institution's environment, and (c) limitations in security features in older or obsolete systems. Effective end-of-life management should include the following: • Maintaining inventories of systems and applications. • Adhering to an approved end-of-life or sunset policy for older systems. • Tracking changes made to the systems and applications, availability of updates, and the planned end of support by the vendor. • Conducting risk assessments on systems and applications to help determine end-of-life. • Planning for the replacement of systems nearing obsolescence and complying with policy requirements for implementing new systems or applications. • Developing specific procedures for the secure destruction or data wiping of hard drives returned to vendors or donated, to prevent the inadvertent disclosure of sensitive information. If an end-of-life system or application must remain in use, management should ensure appropriate mitigating controls are in place, which may include segregating the system or application from the network. Management should also have a plan to replace the system or application and implement compensating	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5		DCH-09
II.C.12	N/A	Malware Mitigation Attackers use malware to obtain access to an institution's environment and to execute an attack within the environment. Malware may enter through public or private networks and from devices attached to the network. Although protective mechanisms may block most malware before it does damage, even a single malicious executable34 may create a significant potential for loss. Management should implement defense-in-depth to protect, detect, and respond to malware. The institution can use many tools to block malware before it enters the environment and to detect it and respond if it is not blocked. Methods or systems that management should consider include the following: • Hardware-based roots of trust, which use cryptographic means to verify the integrity of software. • Servers that run active content at the gateway and disallow content based on policy. • Blacklists that disallow code execution based on code fragments, Internet locations, and other factors that correlate with malicious code. • White lists of allowed programs. • Port monitoring to identify unauthorized network connections. • Network segregation. • Computer configuration to permit the least amount of privileges necessary to perform the user's job. • Application sandboxing35 to limit the access and functionality of executed code. • Monitoring for unauthorized software and disallowing the ability to install unauthorized software. • Monitoring for anomalous activity for malware and polymorphic code. • Monitoring of network traffic. • User education in awareness, safe computing practices, indicators of malicious code, and response actions.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5		CFG-03.3
II.C.12	N/A	Malware Mitigation Attackers use malware to obtain access to an institution's environment and to execute an attack within the environment. Malware may enter through public or private networks and from devices attached to the network. Although protective mechanisms may block most malware before it does damage, even a single malicious executable34 may create a significant potential for loss. Management should implement defense-in-depth to protect, detect, and respond to malware. The institution can use many tools to block malware before it enters the environment and to detect it and respond if it is not blocked. Methods or systems that management should consider include the following: • Hardware-based roots of trust, which use cryptographic means to verify the integrity of software. • Servers that run active content at the gateway and disallow content based on policy. • Blacklists that disallow code execution based on code fragments, Internet locations, and other factors that correlate with malicious code. • White lists of allowed programs. • Port monitoring to identify unauthorized network connections. • Network segregation. • Computer configuration to permit the least amount of privileges necessary to perform the user's job. • Application sandboxing35 to limit the access and functionality of executed code. • Monitoring for unauthorized software and disallowing the ability to install unauthorized software. • Monitoring for anomalous activity for malware and polymorphic code. • Monitoring of network traffic. • User education in awareness, safe computing practices, indicators of malicious code, and response actions.	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
II.C.12	N/A	Malware Mitigation Attackers use malware to obtain access to an institution's environment and to execute an attack within the environment. Malware may enter through public or private networks and from devices attached to the network. Although protective mechanisms may block most malware before it does damage, even a single malicious executable34 may create a significant potential for loss. Management should implement defense-in-depth to protect, detect, and respond to malware. The institution can use many tools to block malware before it enters the environment and to detect it and respond if it is not blocked. Methods or systems that management should consider include the following: • Hardware-based roots of trust, which use cryptographic means to verify the integrity of software. • Servers that run active content at the gateway and disallow content based on policy. • Blacklists that disallow code execution based on code fragments, Internet locations, and other factors that correlate with malicious code. • White lists of allowed programs. • Port monitoring to identify unauthorized network connections. • Network segregation. • Computer configuration to permit the least amount of privileges necessary to perform the user's job. • Application sandboxing35 to limit the access and functionality of executed code. • Monitoring for unauthorized software and disallowing the ability to install unauthorized software. • Monitoring for anomalous activity for malware and polymorphic code. • Monitoring of network traffic. • User education in awareness, safe computing practices, indicators of malicious code, and response actions.	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.	3		NET-06

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.12	N/A	Malware Mitigation Attackers use malware to obtain access to an institution's environment and to execute an attack within the environment. Malware may enter through public or private networks and from devices attached to the network. Although protective mechanisms may block most malware before it does damage, even a single malicious executable34 may create a significant potential for loss. Management should implement defense-in-depth to protect, detect, and respond to malware. The institution can use many tools to block malware before it enters the environment and to detect it and respond if it is not blocked. Methods or systems that management should consider include the following: • Hardware-based roots of trust, which use cryptographic means to verify the integrity of software. • Servers that run active content at the gateway and disallow content based on policy. • Blacklists that disallow code execution based on code fragments, Internet locations, and other factors that correlate with malicious code. • White lists of allowed programs. • Port monitoring to identify unauthorized network connections. • Network segregation. • Computer configuration to permit the least amount of privileges necessary to perform the user's job. • Application sandboxing35 to limit the access and functionality of executed code. • Monitoring for unauthorized software and disallowing the ability to install unauthorized software. • Monitoring for anomalous activity for malware and polymorphic code. • Monitoring of network traffic. • User education in awareness, safe computing practices, indicators of malicious code, and response actions.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-06.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5		SAT-03.2
II.C.13	Encryption	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.C.13.a	N/A	Management should implement policies to govern the secure storage of all types of sensitive information, whether on computer systems, on physical media, or in hard-copy documents. Management can achieve secure storage with physical controls,36 logical controls (e.g., passwords, tokens, and biometrics), and environmental controls (e.g., fire and flood protection). In addition, stored information, in any form, should be classified and inventoried so that it can be retrieved when needed. Inventories should be updated periodically to remain current. More sensitive information, such as system documentation, application source code, and production transaction data, should have more extensive controls to guard against alteration (e.g., integrity checkers and cryptographic hashes). Management should have appropriate logging and monitoring controls over stored information to ensure authorized access and appropriate use. Periodically, the security staff, audit staff, and data owners should review access rights to ensure the access rights remain appropriate and current. Data storage in portable devices, such as laptops, smart phones, and tablets, poses unique problems. These devices may be lost, stolen, or subject to unauthorized and undetected use. Risk mitigation typically involves data encryption, host-provided access controls, homing beacons,37 and remote deletion38 capabilities. Management should implement appropriate controls (such as the use of a DLP program) over portable devices and the sensitive information contained on them. Many institutions create or use a third-party cloud for storage. Cloud storage39 provides unique issues and challenges. Management should understand the nature of the cloud technology being used; the physical location(s) where the data are stored and related legal jurisdiction; the access controls used and protection of the institution's data (e.g., how access is controlled and how that information is retrieved); and the frequency and method of backup used	Functional	Intersects With	Sensitive Data In Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive and/or regulated data in public cloud providers.	5		CLD-10
II.C.13.a	N/A	Management should implement policies to govern the secure storage of all types of sensitive information, whether on computer systems, on physical media, or in hard-copy documents. Management can achieve secure storage with physical controls,36 logical controls (e.g., passwords, tokens, and biometrics), and environmental controls (e.g., fire and flood protection). In addition, stored information, in any form, should be classified and inventoried so that it can be retrieved when needed. Inventories should be updated periodically to remain current. More sensitive information, such as system documentation, application source code, and production transaction data, should have more extensive controls to guard against alteration (e.g., integrity checkers and cryptographic hashes). Management should have appropriate logging and monitoring controls over stored information to ensure authorized access and appropriate use. Periodically, the security staff, audit staff, and data owners should review access rights to ensure the access rights remain appropriate and current. Data storage in portable devices, such as laptops, smart phones, and tablets, poses unique problems. These devices may be lost, stolen, or subject to unauthorized and undetected use. Risk mitigation typically involves data encryption, host-provided access controls, homing beacons,37 and remote deletion38 capabilities. Management should implement appropriate controls (such as the use of a DLP program) over portable devices and the sensitive information contained on them. Many institutions create or use a third-party cloud for storage. Cloud storage39 provides unique issues and challenges. Management should understand the nature of the cloud technology being used; the physical location(s) where the data are stored and related legal jurisdiction; the access controls used and protection of the institution's data (e.g., how access is controlled and how that information is retrieved); and the frequency and method of backup used	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-07	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5		DCH-01.2
II.C.13.a	N/A	Management should implement policies to govern the secure storage of all types of sensitive information, whether on computer systems, on physical media, or in hard-copy documents. Management can achieve secure storage with physical controls,36 logical controls (e.g., passwords, tokens, and biometrics), and environmental controls (e.g., fire and flood protection). In addition, stored information, in any form, should be classified and inventoried so that it can be retrieved when needed. Inventories should be updated periodically to remain current. More sensitive information, such as system documentation, application source code, and production transaction data, should have more extensive controls to guard against alteration (e.g., integrity checkers and cryptographic hashes). Management should have appropriate logging and monitoring controls over stored information to ensure authorized access and appropriate use. Periodically, the security staff, audit staff, and data owners should review access rights to ensure the access rights remain appropriate and current. Data storage in portable devices, such as laptops, smart phones, and tablets, poses unique problems. These devices may be lost, stolen, or subject to unauthorized and undetected use. Risk mitigation typically involves data encryption, host-provided access controls, homing beacons,37 and remote deletion38 capabilities. Management should implement appropriate controls (such as the use of a DLP program) over portable devices and the sensitive information contained on them. Many institutions create or use a third-party cloud for storage. Cloud storage39 provides unique issues and challenges. Management should understand the nature of the cloud technology being used; the physical location(s) where the data are stored and related legal jurisdiction; the access controls used and protection of the institution's data (e.g., how access is controlled and how that information is retrieved); and the frequency and method of backup used	Functional	Intersects With	Media Storage	DCH-13	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5		DCH-06

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.13.a	N/A	Management should implement policies to govern the secure storage of all types of sensitive information, whether on computer systems, on physical media, or in hard-copy documents. Management can achieve secure storage with physical controls,36 logical controls (e.g., passwords, tokens, and biometrics), and environmental controls (e.g., fire and flood protection). In addition, stored information, in any form, should be classified and inventoried so that it can be retrieved when needed. Inventories should be updated periodically to remain current. More sensitive information, such as system documentation, application source code, and production transaction data, should have more extensive controls to guard against alteration (e.g., integrity checkers and cryptographic hashes). Management should have appropriate logging and monitoring controls over stored information to ensure authorized access and appropriate use. Periodically, the security staff, audit staff, and data owners should review access rights to ensure the access rights remain appropriate and current. Data storage in portable devices, such as laptops, smart phones, and tablets, poses unique problems. These devices may be lost, stolen, or subject to unauthorized and undetected use. Risk mitigation typically involves data encryption, host-provided access controls, homing beacons,37 and remote deletion38 capabilities. Management should implement appropriate controls (such as the use of a DLP program) over portable devices and the sensitive information contained on them. Many institutions create or use a third-party cloud for storage. Cloud storage39 provides unique issues and challenges. Management should understand the nature of the cloud technology being used; the physical location(s) where the data are stored and related legal jurisdiction; the access controls used and protection of the institution's data (e.g., how access is controlled and how that information is retrieved); and the frequency and method of backup used	Functional	Intersects With	Data Loss Prevention (DLP)	DCH-40	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	3		NET-17
II.C.13.a	N/A	Management should implement policies to govern the secure storage of all types of sensitive information, whether on computer systems, on physical media, or in hard-copy documents. Management can achieve secure storage with physical controls,36 logical controls (e.g., passwords, tokens, and biometrics), and environmental controls (e.g., fire and flood protection). In addition, stored information, in any form, should be classified and inventoried so that it can be retrieved when needed. Inventories should be updated periodically to remain current. More sensitive information, such as system documentation, application source code, and production transaction data, should have more extensive controls to guard against alteration (e.g., integrity checkers and cryptographic hashes). Management should have appropriate logging and monitoring controls over stored information to ensure authorized access and appropriate use. Periodically, the security staff, audit staff, and data owners should review access rights to ensure the access rights remain appropriate and current. Data storage in portable devices, such as laptops, smart phones, and tablets, poses unique problems. These devices may be lost, stolen, or subject to unauthorized and undetected use. Risk mitigation typically involves data encryption, host-provided access controls, homing beacons,37 and remote deletion38 capabilities. Management should implement appropriate controls (such as the use of a DLP program) over portable devices and the sensitive information contained on them. Many institutions create or use a third-party cloud for storage. Cloud storage39 provides unique issues and challenges. Management should understand the nature of the cloud technology being used; the physical location(s) where the data are stored and related legal jurisdiction; the access controls used and protection of the institution's data (e.g., how access is controlled and how that information is retrieved); and the frequency and method of backup used	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-04	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5		MDM-03
II.C.13.b	N/A	Electronic transmission of information can include e-mail, file transfer protocol (FTP), secure FTP (sFTP), secure shell, dedicated line, short message service/texting, and transmission via the Internet. Management should determine the type of transmission method, sensitivity of the 36 Refer to the "Physical Security" section of this booklet. 37 Homing beacons send messages to the institution when they connect to a network and enable recovery of the device. 38 Remote deletion is a technology that enables the institution to remotely delete certain data from a portable device. 39 Cloud storage is a model of data storage in which the digital data are stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. information to be transmitted, and types of safeguards available to protect information. Management should implement appropriate controls or, if they are not available, restrict the type of information that can be transmitted. When transmitting sensitive information over a public network, information should be encrypted to protect it from interception or eavesdropping. Techniques include secure e-mail protocols, sFTP, and secure sockets layer (SSL) certificates.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
II.C.13.b	N/A	Electronic transmission of information can include e-mail, file transfer protocol (FTP), secure FTP (sFTP), secure shell, dedicated line, short message service/texting, and transmission via the Internet. Management should determine the type of transmission method, sensitivity of the 36 Refer to the "Physical Security" section of this booklet. 37 Homing beacons send messages to the institution when they connect to a network and enable recovery of the device. 38 Remote deletion is a technology that enables the institution to remotely delete certain data from a portable device. 39 Cloud storage is a model of data storage in which the digital data are stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. information to be transmitted, and types of safeguards available to protect information. Management should implement appropriate controls or, if they are not available, restrict the type of information that can be transmitted. When transmitting sensitive information over a public network, information should be encrypted to protect it from interception or eavesdropping. Techniques include secure e-mail protocols, sFTP, and secure sockets layer (SSL) certificates.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-37	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive and/or regulated data during transmission over open, public networks.	8		NET-12

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.13.b	N/A	Electronic transmission of information can include e-mail, file transfer protocol (FTP), secure FTP (sFTP), secure shell, dedicated line, short message service/texting, and transmission via the Internet. Management should determine the type of transmission method, sensitivity of the 36 Refer to the "Physical Security" section of this booklet. 37 Homing beacons send messages to the institution when they connect to a network and enable recovery of the device. 38 Remote deletion is a technology that enables the institution to remotely delete certain data from a portable device. 39 Cloud storage is a model of data storage in which the digital data are stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. information to be transmitted, and types of safeguards available to protect information. Management should implement appropriate controls or, if they are not available, restrict the type of information that can be transmitted. When transmitting sensitive information over a public network, information should be encrypted to protect it from interception or eavesdropping. Techniques include secure e-mail protocols, sFTP, and secure sockets layer (SSL) certificates.	Functional	Intersects With	End-User Messaging Technologies	NET-40	Mechanisms exist to prohibit the transmission of unprotected sensitive and/or regulated data by end-user messaging technologies.	5		NET-12.2
II.C.13.c	N/A	Disposal of Information The institution should have appropriate disposal procedures for paper-based and electronic information.40 Designating a single individual, department, or function to be responsible for disposal facilitates accountability and promotes compliance with disposal policies. Policies should prohibit employees from discarding paper-based information containing sensitive information by using the same disposal system as regular garbage to avoid accidental disclosure. Many institutions shred paper-based media on-site while others use collection and disposal services to ensure the media are rendered unreadable and unlikely to be reconstructed. Institutions that contract with third-party service providers should conduct due diligence to ensure those third parties conduct adequate employee background checks and employ appropriate controls. Contracts with third-party disposal firms should address acceptable disposal procedures. Electronic information and computer-based media present distinct disposal challenges. In addition to disk drives and other forms of storage, information frequently is contained in or on the memory of other devices (e.g., printers, fax machines, and cellphones). Residual data frequently remain on media, even after deletion. Because the data can be recovered, additional disposal techniques should be applied to devices containing sensitive data. Overwriting destroys data by replacing it with new, random data. Overwriting may be preferable when the media will be reused. To be effective, overwriting may have to be performed many times. Another disposal technique is degaussing, which scrambles the data recorded on the media with powerful, varying magnetic fields. Physical destruction of the media can make the data unrecoverable. Data can sometimes be destroyed after overwriting. Management should determine the most effective method of disposal based on the type of information. Policies and procedures	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09
II.C.13.c	N/A	Disposal of Information The institution should have appropriate disposal procedures for paper-based and electronic information.40 Designating a single individual, department, or function to be responsible for disposal facilitates accountability and promotes compliance with disposal policies. Policies should prohibit employees from discarding paper-based information containing sensitive information by using the same disposal system as regular garbage to avoid accidental disclosure. Many institutions shred paper-based media on-site while others use collection and disposal services to ensure the media are rendered unreadable and unlikely to be reconstructed. Institutions that contract with third-party service providers should conduct due diligence to ensure those third parties conduct adequate employee background checks and employ appropriate controls. Contracts with third-party disposal firms should address acceptable disposal procedures. Electronic information and computer-based media present distinct disposal challenges. In addition to disk drives and other forms of storage, information frequently is contained in or on the memory of other devices (e.g., printers, fax machines, and cellphones). Residual data frequently remain on media, even after deletion. Because the data can be recovered, additional disposal techniques should be applied to devices containing sensitive data. Overwriting destroys data by replacing it with new, random data. Overwriting may be preferable when the media will be reused. To be effective, overwriting may have to be performed many times. Another disposal technique is degaussing, which scrambles the data recorded on the media with powerful, varying magnetic fields. Physical destruction of the media can make the data unrecoverable. Data can sometimes be destroyed after overwriting. Management should determine the most effective method of disposal based on the type of information. Policies and procedures	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08
II.C.13.c	N/A	Disposal of Information The institution should have appropriate disposal procedures for paper-based and electronic information.40 Designating a single individual, department, or function to be responsible for disposal facilitates accountability and promotes compliance with disposal policies. Policies should prohibit employees from discarding paper-based information containing sensitive information by using the same disposal system as regular garbage to avoid accidental disclosure. Many institutions shred paper-based media on-site while others use collection and disposal services to ensure the media are rendered unreadable and unlikely to be reconstructed. Institutions that contract with third-party service providers should conduct due diligence to ensure those third parties conduct adequate employee background checks and employ appropriate controls. Contracts with third-party disposal firms should address acceptable disposal procedures. Electronic information and computer-based media present distinct disposal challenges. In addition to disk drives and other forms of storage, information frequently is contained in or on the memory of other devices (e.g., printers, fax machines, and cellphones). Residual data frequently remain on media, even after deletion. Because the data can be recovered, additional disposal techniques should be applied to devices containing sensitive data. Overwriting destroys data by replacing it with new, random data. Overwriting may be preferable when the media will be reused. To be effective, overwriting may have to be performed many times. Another disposal technique is degaussing, which scrambles the data recorded on the media with powerful, varying magnetic fields. Physical destruction of the media can make the data unrecoverable. Data can sometimes be destroyed after overwriting. Management should determine the most effective method of disposal based on the type of information. Policies and procedures	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	8		DCH-09

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.13.c	N/A	Disposal of Information The institution should have appropriate disposal procedures for paper-based and electronic information.40 Designating a single individual, department, or function to be responsible for disposal facilitates accountability and promotes compliance with disposal policies. Policies should prohibit employees from discarding paper-based information containing sensitive information by using the same disposal system as regular garbage to avoid accidental disclosure. Many institutions shred paper-based media on-site while others use collection and disposal services to ensure the media are rendered unreadable and unlikely to be reconstructed. Institutions that contract with third-party service providers should conduct due diligence to ensure those third parties conduct adequate employee background checks and employ appropriate controls. Contracts with third-party disposal firms should address acceptable disposal procedures. Electronic information and computer-based media present distinct disposal challenges. In addition to disk drives and other forms of storage, information frequently is contained in or on the memory of other devices (e.g., printers, fax machines, and cellphones). Residual data frequently remain on media, even after deletion. Because the data can be recovered, additional disposal techniques should be applied to devices containing sensitive data. Overwriting destroys data by replacing it with new, random data. Overwriting may be preferable when the media will be reused. To be effective, overwriting may have to be performed many times. Another disposal technique is degaussing, which scrambles the data recorded on the media with powerful, varying magnetic fields. Physical destruction of the media can make the data unrecoverable. Data can sometimes be destroyed after overwriting. Management should determine the most effective method of disposal based on the type of information. Policies and procedures	Functional	Intersects With	Digital Media Sanitization Documentation	DCH-18.2	Mechanisms exist to supervise, track, document and verify digital media sanitization and disposal actions.	5		DCH-09.1
II.C.13.c	N/A	Disposal of Information The institution should have appropriate disposal procedures for paper-based and electronic information.40 Designating a single individual, department, or function to be responsible for disposal facilitates accountability and promotes compliance with disposal policies. Policies should prohibit employees from discarding paper-based information containing sensitive information by using the same disposal system as regular garbage to avoid accidental disclosure. Many institutions shred paper-based media on-site while others use collection and disposal services to ensure the media are rendered unreadable and unlikely to be reconstructed. Institutions that contract with third-party service providers should conduct due diligence to ensure those third parties conduct adequate employee background checks and employ appropriate controls. Contracts with third-party disposal firms should address acceptable disposal procedures. Electronic information and computer-based media present distinct disposal challenges. In addition to disk drives and other forms of storage, information frequently is contained in or on the memory of other devices (e.g., printers, fax machines, and cellphones). Residual data frequently remain on media, even after deletion. Because the data can be recovered, additional disposal techniques should be applied to devices containing sensitive data. Overwriting destroys data by replacing it with new, random data. Overwriting may be preferable when the media will be reused. To be effective, overwriting may have to be performed many times. Another disposal technique is degaussing, which scrambles the data recorded on the media with powerful, varying magnetic fields. Physical destruction of the media can make the data unrecoverable. Data can sometimes be destroyed after overwriting. Management should determine the most effective method of disposal based on the type of information. Policies and procedures	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
II.C.13.d	N/A	Management should implement policies for maintaining the security of physical media (including backup tapes) containing sensitive information while in transit, including to off-site storage, or when shared with third parties. Policies should include the following: • Contractual requirements that incorporate necessary risk-based controls. • Restrictions on the carriers used. • Procedures to verify the identity of couriers. • Requirements for appropriate packaging to protect the media from damage. • Use of adequate encryption of sensitive information recorded on media that is being physically transported. • Tracking of shipments to provide early indications of loss or damage. • Security reviews or independent security reports of receiving companies. • Use of nondisclosure agreements for couriers	Functional	Intersects With	Management Approval For External Media Transfer	AST-18.1	Mechanisms exist to obtain management approval for any sensitive and/or regulated media that is transferred outside of the organization's facilities.	3		AST-05.1
II.C.13.d	N/A	Management should implement policies for maintaining the security of physical media (including backup tapes) containing sensitive information while in transit, including to off-site storage, or when shared with third parties. Policies should include the following: • Contractual requirements that incorporate necessary risk-based controls. • Restrictions on the carriers used. • Procedures to verify the identity of couriers. • Requirements for appropriate packaging to protect the media from damage. • Use of adequate encryption of sensitive information recorded on media that is being physically transported. • Tracking of shipments to provide early indications of loss or damage. • Security reviews or independent security reports of receiving companies. • Use of nondisclosure agreements for couriers	Functional	Intersects With	Media Transportation	DCH-16	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	8		DCH-07
II.C.13.d	N/A	Management should implement policies for maintaining the security of physical media (including backup tapes) containing sensitive information while in transit, including to off-site storage, or when shared with third parties. Policies should include the following: • Contractual requirements that incorporate necessary risk-based controls. • Restrictions on the carriers used. • Procedures to verify the identity of couriers. • Requirements for appropriate packaging to protect the media from damage. • Use of adequate encryption of sensitive information recorded on media that is being physically transported. • Tracking of shipments to provide early indications of loss or damage. • Security reviews or independent security reports of receiving companies. • Use of nondisclosure agreements for couriers	Functional	Intersects With	Media Transportation Custodians	DCH-16.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5		DCH-07.1
II.C.13.d	N/A	Management should implement policies for maintaining the security of physical media (including backup tapes) containing sensitive information while in transit, including to off-site storage, or when shared with third parties. Policies should include the following: • Contractual requirements that incorporate necessary risk-based controls. • Restrictions on the carriers used. • Procedures to verify the identity of couriers. • Requirements for appropriate packaging to protect the media from damage. • Use of adequate encryption of sensitive information recorded on media that is being physically transported. • Tracking of shipments to provide early indications of loss or damage. • Security reviews or independent security reports of receiving companies. • Use of nondisclosure agreements for couriers	Functional	Intersects With	Encrypting Data Outside of Controlled Areas	DCH-16.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5		DCH-07.2
II.C.13.e	N/A	Rogue or Shadow IT Management should have policies explaining that employees should not and are not authorized to use unsanctioned or unapproved IT resources (e.g., online storage services, unapproved mobile device applications, and unapproved devices). Security awareness or information security training should include procedures for identifying and reporting shadow IT.	Functional	Intersects With	Approved Technologies	AST-10	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5		AST-01.4

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.13.e	N/A	Rogue or Shadow IT Management should have policies explaining that employees should not and are not authorized to use unsanctioned or unapproved IT resources (e.g., online storage services, unapproved mobile device applications, and unapproved devices). Security awareness or information security training should include procedures for identifying and reporting shadow IT.	Functional	Intersects With	Technology Use Restrictions	HRS-06.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5		HRS-05.3
II.C.13.e	N/A	Rogue or Shadow IT Management should have policies explaining that employees should not and are not authorized to use unsanctioned or unapproved IT resources (e.g., online storage services, unapproved mobile device applications, and unapproved devices). Security awareness or information security training should include procedures for identifying and reporting shadow IT.	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
II.C.13.e	N/A	Rogue or Shadow IT Management should have policies explaining that employees should not and are not authorized to use unsanctioned or unapproved IT resources (e.g., online storage services, unapproved mobile device applications, and unapproved devices). Security awareness or information security training should include procedures for identifying and reporting shadow IT.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3		SAT-02
II.C.14	N/A	Supply Chain The typical institution purchases a wide variety of hardware and software, which often is manufactured or developed internationally. In a supply chain attack, a threat source incorporates unidentified and harmful features into the purchased items before delivery. During the risk identification process, management should identify factors that may increase risk from supply chain attacks and respond with appropriate risk mitigations. An effective information security program seeks to limit the potential for harm through techniques tailored to specific acquisitions and services. Examples of techniques to mitigate the risk from such attacks include the following: • Only making purchases through reputable sellers who demonstrate an ability to control their own supply chains. • Purchasing hardware and software through third parties to shield the institution's identity. • Reviewing hardware for anomalies. • Using automated software testing and code reviews for software. • Regularly reviewing the reliability of software and hardware items purchased through activity monitoring and evaluations by user groups.	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1
II.C.14	N/A	Supply Chain The typical institution purchases a wide variety of hardware and software, which often is manufactured or developed internationally. In a supply chain attack, a threat source incorporates unidentified and harmful features into the purchased items before delivery. During the risk identification process, management should identify factors that may increase risk from supply chain attacks and respond with appropriate risk mitigations. An effective information security program seeks to limit the potential for harm through techniques tailored to specific acquisitions and services. Examples of techniques to mitigate the risk from such attacks include the following: • Only making purchases through reputable sellers who demonstrate an ability to control their own supply chains. • Purchasing hardware and software through third parties to shield the institution's identity. • Reviewing hardware for anomalies. • Using automated software testing and code reviews for software. • Regularly reviewing the reliability of software and hardware items purchased through activity monitoring and evaluations by user groups.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-09	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	3		TDA-11
II.C.14	N/A	Supply Chain The typical institution purchases a wide variety of hardware and software, which often is manufactured or developed internationally. In a supply chain attack, a threat source incorporates unidentified and harmful features into the purchased items before delivery. During the risk identification process, management should identify factors that may increase risk from supply chain attacks and respond with appropriate risk mitigations. An effective information security program seeks to limit the potential for harm through techniques tailored to specific acquisitions and services. Examples of techniques to mitigate the risk from such attacks include the following: • Only making purchases through reputable sellers who demonstrate an ability to control their own supply chains. • Purchasing hardware and software through third parties to shield the institution's identity. • Reviewing hardware for anomalies. • Using automated software testing and code reviews for software. • Regularly reviewing the reliability of software and hardware items purchased through activity monitoring and evaluations by user groups.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	8		TPM-03
II.C.14	N/A	Supply Chain The typical institution purchases a wide variety of hardware and software, which often is manufactured or developed internationally. In a supply chain attack, a threat source incorporates unidentified and harmful features into the purchased items before delivery. During the risk identification process, management should identify factors that may increase risk from supply chain attacks and respond with appropriate risk mitigations. An effective information security program seeks to limit the potential for harm through techniques tailored to specific acquisitions and services. Examples of techniques to mitigate the risk from such attacks include the following: • Only making purchases through reputable sellers who demonstrate an ability to control their own supply chains. • Purchasing hardware and software through third parties to shield the institution's identity. • Reviewing hardware for anomalies. • Using automated software testing and code reviews for software. • Regularly reviewing the reliability of software and hardware items purchased through activity monitoring and evaluations by user groups.	Functional	Intersects With	Limit Potential Harm	TPM-04.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5		TPM-03.2
II.C.15	Access Governance	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.C.15.a	N/A	Access to the operating system and system utilities provide users with the authority to make fundamental changes to the system. System utilities are programs that perform repetitive functions, such as creating, deleting, changing, or copying files. System utilities also could include numerous types of system management software that can supplement operating system functionality by supporting common system tasks, such as security, system monitoring, or transaction processing. Unauthorized access to the operating system and system utilities could result in significant financial and operational losses. System and security administrators should restrict and monitor privileged access to operating systems and system utilities. Many operating systems have integrated or third-party access control software, which is often essential to effective access control and can be used to integrate the security management of the operating system and applications. To prevent unauthorized access to or inappropriate activity on the operating system and system utilities, management should do the following: • Implement effective user access to appropriately restrict system access for both users and applications and, depending on the sensitivity, extend protection at the program, file, record, or field level. • Limit the number of employees with access to operating systems and grant only the minimum level of access required to perform job responsibilities. • Restrict and log access to and activity on operating system parameters, system utilities (especially those with data-altering capabilities), and sensitive system resources (including files, programs, and processes), and supplement with additional security software, as necessary. • Restrict operating system access to specific terminals in physically secure and monitored locations. • Secure or remove external drives and portable media from system consoles, terminals, or personal computers (PC) running terminal emulations, residing outside of physically secure locations. •	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

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.15.a	N/A	Access to the operating system and system utilities provide users with the authority to make fundamental changes to the system. System utilities are programs that perform repetitive functions, such as creating, deleting, changing, or copying files. System utilities also could include numerous types of system management software that can supplement operating system functionality by supporting common system tasks, such as security, system monitoring, or transaction processing. Unauthorized access to the operating system and system utilities could result in significant financial and operational losses. System and security administrators should restrict and monitor privileged access to operating systems and system utilities. Many operating systems have integrated or third-party access control software, which is often essential to effective access control and can be used to integrate the security management of the operating system and applications. To prevent unauthorized access to or inappropriate activity on the operating system and system utilities, management should do the following: • Implement effective user access to appropriately restrict system access for both users and applications and, depending on the sensitivity, extend protection at the program, file, record, or field level. • Limit the number of employees with access to operating systems and grant only the minimum level of access required to perform job responsibilities. • Restrict and log access to and activity on operating system parameters, system utilities (especially those with data-altering capabilities), and sensitive system resources (including files, programs, and processes), and supplement with additional security software, as necessary. • Restrict operating system access to specific terminals in physically secure and monitored locations. • Secure or remove external drives and portable media from system consoles, terminals, or personal computers (PC) running terminal emulations, residing outside of physically secure locations. •	Functional	Intersects With	Use of Privileged Utility Programs	IAC-26	Mechanisms exist to restrict and tightly control utility programs that are capable of overriding system and application controls.	8		IAC-20.3
II.C.15.a	N/A	Access to the operating system and system utilities provide users with the authority to make fundamental changes to the system. System utilities are programs that perform repetitive functions, such as creating, deleting, changing, or copying files. System utilities also could include numerous types of system management software that can supplement operating system functionality by supporting common system tasks, such as security, system monitoring, or transaction processing. Unauthorized access to the operating system and system utilities could result in significant financial and operational losses. System and security administrators should restrict and monitor privileged access to operating systems and system utilities. Many operating systems have integrated or third-party access control software, which is often essential to effective access control and can be used to integrate the security management of the operating system and applications. To prevent unauthorized access to or inappropriate activity on the operating system and system utilities, management should do the following: • Implement effective user access to appropriately restrict system access for both users and applications and, depending on the sensitivity, extend protection at the program, file, record, or field level. • Limit the number of employees with access to operating systems and grant only the minimum level of access required to perform job responsibilities. • Restrict and log access to and activity on operating system parameters, system utilities (especially those with data-altering capabilities), and sensitive system resources (including files, programs, and processes), and supplement with additional security software, as necessary. • Restrict operating system access to specific terminals in physically secure and monitored locations. • Secure or remove external drives and portable media from system consoles, terminals, or personal computers (PC) running terminal emulations, residing outside of physically secure locations. •	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 functions.	5		IAC-21
II.C.15.a	N/A	Access to the operating system and system utilities provide users with the authority to make fundamental changes to the system. System utilities are programs that perform repetitive functions, such as creating, deleting, changing, or copying files. System utilities also could include numerous types of system management software that can supplement operating system functionality by supporting common system tasks, such as security, system monitoring, or transaction processing. Unauthorized access to the operating system and system utilities could result in significant financial and operational losses. System and security administrators should restrict and monitor privileged access to operating systems and system utilities. Many operating systems have integrated or third-party access control software, which is often essential to effective access control and can be used to integrate the security management of the operating system and applications. To prevent unauthorized access to or inappropriate activity on the operating system and system utilities, management should do the following: • Implement effective user access to appropriately restrict system access for both users and applications and, depending on the sensitivity, extend protection at the program, file, record, or field level. • Limit the number of employees with access to operating systems and grant only the minimum level of access required to perform job responsibilities. • Restrict and log access to and activity on operating system parameters, system utilities (especially those with data-altering capabilities), and sensitive system resources (including files, programs, and processes), and supplement with additional security software, as necessary. • Restrict operating system access to specific terminals in physically secure and monitored locations. • Secure or remove external drives and portable media from system consoles, terminals, or personal computers (PC) running terminal emulations, residing outside of physically secure locations. •	Functional	Intersects With	Privileged Functions Logging	MON-14	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5		MON-03.3
II.C.15.b	N/A	Sensitive or mission-critical applications should incorporate appropriate access controls that restrict which functions are available to users and other applications. These access controls allow authorized users and other applications to interface with related databases. Some security software programs integrate access control between the operating system and some applications. Such software is useful when applications do not have their own access controls or when the institution uses security software instead of the application's native access controls. Management should understand the functionality and vulnerabilities of the application access control solutions and consider those issues in the risk management process. Management should implement effective application access controls by doing the following: • Implementing a robust authentication41 method consistent with the criticality and sensitivity of the application. • Easing the administrative burden of managing application access rights by using group profiles. Managing access rights individually can lead to inconsistent or inappropriate access levels. • Periodically reviewing and approving the application access assigned to users for appropriateness. • Communicating and enforcing the responsibilities of programmers, security administrators, and application owners for maintaining effective application access control. • Setting time-of-day or terminal limitations for some applications or for more sensitive functions within an application. • Logging access and events, defining alerts for significant events, and developing processes to monitor and respond to anomalies and alerts.	Functional	Intersects With	Attribute-Based Access Control (ABAC)	IAC-07	Automated mechanisms exist to enforce Attribute-Based Access Control (ABAC) through policy-driven, dynamic authorizations to: (1) Enforce usage conditions for users and/or role; and (2) Support the secure sharing of information.	3		IAC-15.8

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.15.b	N/A	Sensitive or mission-critical applications should incorporate appropriate access controls that restrict which functions are available to users and other applications. These access controls allow authorized users and other applications to interface with related databases. Some security software programs integrate access control between the operating system and some applications. Such software is useful when applications do not have their own access controls or when the institution uses security software instead of the application's native access controls. Management should understand the functionality and vulnerabilities of the application access control solutions and consider those issues in the risk management process. Management should implement effective application access controls by doing the following: • Implementing a robust authentication41 method consistent with the criticality and sensitivity of the application. • Easing the administrative burden of managing application access rights by using group profiles. Managing access rights individually can lead to inconsistent or inappropriate access levels. • Periodically reviewing and approving the application access assigned to users for appropriateness. • Communicating and enforcing the responsibilities of programmers, security administrators, and application owners for maintaining effective application access control. • Setting time-of-day or terminal limitations for some applications or for more sensitive functions within an application. • Logging access and events, defining alerts for significant events, and developing processes to monitor and respond to anomalies and alerts.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5		IAC-17
II.C.15.b	N/A	Sensitive or mission-critical applications should incorporate appropriate access controls that restrict which functions are available to users and other applications. These access controls allow authorized users and other applications to interface with related databases. Some security software programs integrate access control between the operating system and some applications. Such software is useful when applications do not have their own access controls or when the institution uses security software instead of the application's native access controls. Management should understand the functionality and vulnerabilities of the application access control solutions and consider those issues in the risk management process. Management should implement effective application access controls by doing the following: • Implementing a robust authentication41 method consistent with the criticality and sensitivity of the application. • Easing the administrative burden of managing application access rights by using group profiles. Managing access rights individually can lead to inconsistent or inappropriate access levels. • Periodically reviewing and approving the application access assigned to users for appropriateness. • Communicating and enforcing the responsibilities of programmers, security administrators, and application owners for maintaining effective application access control. • Setting time-of-day or terminal limitations for some applications or for more sensitive functions within an application. • Logging access and events, defining alerts for significant events, and developing processes to monitor and respond to anomalies and alerts.	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5		IAC-10
II.C.15.b	N/A	Sensitive or mission-critical applications should incorporate appropriate access controls that restrict which functions are available to users and other applications. These access controls allow authorized users and other applications to interface with related databases. Some security software programs integrate access control between the operating system and some applications. Such software is useful when applications do not have their own access controls or when the institution uses security software instead of the application's native access controls. Management should understand the functionality and vulnerabilities of the application access control solutions and consider those issues in the risk management process. Management should implement effective application access controls by doing the following: • Implementing a robust authentication41 method consistent with the criticality and sensitivity of the application. • Easing the administrative burden of managing application access rights by using group profiles. Managing access rights individually can lead to inconsistent or inappropriate access levels. • Periodically reviewing and approving the application access assigned to users for appropriateness. • Communicating and enforcing the responsibilities of programmers, security administrators, and application owners for maintaining effective application access control. • Setting time-of-day or terminal limitations for some applications or for more sensitive functions within an application. • Logging access and events, defining alerts for significant events, and developing processes to monitor and respond to anomalies and alerts.	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		IAC-20
II.C.15.c	N/A	Remote Access Management should develop policies to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner. Such policies and procedures should define how the institution provides remote access and the controls necessary to offer remote access securely. Management should employ the following measures: • Disable remote communications if no business need exists. • Tightly control remote access through management approvals and subsequent audits. • Implement robust controls over configurations at both ends of the remote connection to prevent potential malicious use. • Log and monitor all remote access communications. • Secure remote access devices. • Restrict remote access during specific times. • Limit the applications available for remote access. • Use robust authentication methods for access and encryption to secure communications. There are several methods to provide remote access to employees. A prevalent form of remote access is through a VPN, which provides employees with a remote connection to the institution's network through a secure channel. The VPN connection uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure 41 Stronger authentication and layered security methods, such as the use of tokens, public-key infrastructure-based systems, or out-of-band verification coupled with a robust identity and access management process, can reduce the potential for unauthorized access. access to their organization's network. VPN provides an encrypted isolated "tunnel" or connection between a remote user's computer and the internal network. Because VPN connections provide access to sensitive internal networks, the connections require additional authentication from the remote user. Use of physical token devices is a common method that can provide one-time passwords to strongly	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.	5		IAC-06

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.15.c	N/A	Remote Access Management should develop policies to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner. Such policies and procedures should define how the institution provides remote access and the controls necessary to offer remote access securely. Management should employ the following measures: • Disable remote communications if no business need exists. • Tightly control remote access through management approvals and subsequent audits. • Implement robust controls over configurations at both ends of the remote connection to prevent potential malicious use. • Log and monitor all remote access communications. • Secure remote access devices. • Restrict remote access during specific times. • Limit the applications available for remote access. • Use robust authentication methods for access and encryption to secure communications. There are several methods to provide remote access to employees. A prevalent form of remote access is through a VPN, which provides employees with a remote connection to the institution's network through a secure channel. The VPN connection uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure 41 Stronger authentication and layered security methods, such as the use of tokens, public-key infrastructure-based systems, or out-of-band verification coupled with a robust identity and access management process, can reduce the potential for unauthorized access. access to their organization's network. VPN provides an encrypted isolated "tunnel" or connection between a remote user's computer and the internal network. Because VPN connections provide access to sensitive internal networks, the connections require additional authentication from the remote user. Use of physical token devices is a common method that can provide one-time passwords to strongly	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	8		NET-14
II.C.15.c	N/A	Remote Access Management should develop policies to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner. Such policies and procedures should define how the institution provides remote access and the controls necessary to offer remote access securely. Management should employ the following measures: • Disable remote communications if no business need exists. • Tightly control remote access through management approvals and subsequent audits. • Implement robust controls over configurations at both ends of the remote connection to prevent potential malicious use. • Log and monitor all remote access communications. • Secure remote access devices. • Restrict remote access during specific times. • Limit the applications available for remote access. • Use robust authentication methods for access and encryption to secure communications. There are several methods to provide remote access to employees. A prevalent form of remote access is through a VPN, which provides employees with a remote connection to the institution's network through a secure channel. The VPN connection uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure 41 Stronger authentication and layered security methods, such as the use of tokens, public-key infrastructure-based systems, or out-of-band verification coupled with a robust identity and access management process, can reduce the potential for unauthorized access. access to their organization's network. VPN provides an encrypted isolated "tunnel" or connection between a remote user's computer and the internal network. Because VPN connections provide access to sensitive internal networks, the connections require additional authentication from the remote user. Use of physical token devices is a common method that can provide one-time passwords to strongly	Functional	Intersects With	Remote Access Monitoring & Control	NET-26.4	Automated mechanisms exist to monitor and control remote access sessions.	5		NET-14.1
II.C.15.c	N/A	Remote Access Management should develop policies to ensure that remote access by employees, whether using institution or personally owned devices, is provided in a safe and sound manner. Such policies and procedures should define how the institution provides remote access and the controls necessary to offer remote access securely. Management should employ the following measures: • Disable remote communications if no business need exists. • Tightly control remote access through management approvals and subsequent audits. • Implement robust controls over configurations at both ends of the remote connection to prevent potential malicious use. • Log and monitor all remote access communications. • Secure remote access devices. • Restrict remote access during specific times. • Limit the applications available for remote access. • Use robust authentication methods for access and encryption to secure communications. There are several methods to provide remote access to employees. A prevalent form of remote access is through a VPN, which provides employees with a remote connection to the institution's network through a secure channel. The VPN connection uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure 41 Stronger authentication and layered security methods, such as the use of tokens, public-key infrastructure-based systems, or out-of-band verification coupled with a robust identity and access management process, can reduce the potential for unauthorized access. access to their organization's network. VPN provides an encrypted isolated "tunnel" or connection between a remote user's computer and the internal network. Because VPN connections provide access to sensitive internal networks, the connections require additional authentication from the remote user. Use of physical token devices is a common method that can provide one-time passwords to strongly	Functional	Intersects With	Remote Access Cryptographic Protections	NET-26.5	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	5		NET-14.2

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.15.d	N/A	Management may choose to allow employees to connect remotely to the institution's network using either an institution-owned or a personally owned device (often referred to as BYOD or "bring your own device"). Institution-owned devices are easier to secure because the institution controls the devices' configuration and often can implement remote wiping if the devices are lost or stolen. It may be more difficult to implement remote wiping or a similar measure on an employee's personally owned device. BYOD is becoming more popular, however, with institutions and employees because it reduces costs to the institution and enables employees to carry one device instead of two. For all remote devices, management should do the following to control employee remote access to the institution's network: • Disallow remote access unless a compelling business justification exists. • Require management approval of employee remote access. • Regularly review remote access approvals and rescind those that no longer have a compelling business justification. • Restrict remote access to authorized network areas and applications by using VLANs, permissions, and other techniques. • Log remote access communications (including date, time, user, user location, duration, and activity), analyze logs in a timely manner, and follow up on anomalies. • Implement robust authentication methods for remote access. • Use encryption to protect communications between the access device and the institution. • Use application white-listing.42 For institution-owned devices, the institution should have the ability to manage the remote devices. The following controls should be implemented: • Securely configure remote access devices. • Protect remote access devices against malware. • Patch, update, and maintain all software on remote access devices. • Encrypt sensitive data residing on the access device. • Implement secure containers with internal boundaries to store sensitive information, in a way that is not	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-27	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5		AST-16
II.C.15.d	N/A	Management may choose to allow employees to connect remotely to the institution's network using either an institution-owned or a personally owned device (often referred to as BYOD or "bring your own device"). Institution-owned devices are easier to secure because the institution controls the devices' configuration and often can implement remote wiping if the devices are lost or stolen. It may be more difficult to implement remote wiping or a similar measure on an employee's personally owned device. BYOD is becoming more popular, however, with institutions and employees because it reduces costs to the institution and enables employees to carry one device instead of two. For all remote devices, management should do the following to control employee remote access to the institution's network: • Disallow remote access unless a compelling business justification exists. • Require management approval of employee remote access. • Regularly review remote access approvals and rescind those that no longer have a compelling business justification. • Restrict remote access to authorized network areas and applications by using VLANs, permissions, and other techniques. • Log remote access communications (including date, time, user, user location, duration, and activity), analyze logs in a timely manner, and follow up on anomalies. • Implement robust authentication methods for remote access. • Use encryption to protect communications between the access device and the institution. • Use application white-listing.42 For institution-owned devices, the institution should have the ability to manage the remote devices. The following controls should be implemented: • Securely configure remote access devices. • Protect remote access devices against malware. • Patch, update, and maintain all software on remote access devices. • Encrypt sensitive data residing on the access device. • Implement secure containers with internal boundaries to store sensitive information, in a way that is not	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5		MDM-01
II.C.15.d	N/A	Management may choose to allow employees to connect remotely to the institution's network using either an institution-owned or a personally owned device (often referred to as BYOD or "bring your own device"). Institution-owned devices are easier to secure because the institution controls the devices' configuration and often can implement remote wiping if the devices are lost or stolen. It may be more difficult to implement remote wiping or a similar measure on an employee's personally owned device. BYOD is becoming more popular, however, with institutions and employees because it reduces costs to the institution and enables employees to carry one device instead of two. For all remote devices, management should do the following to control employee remote access to the institution's network: • Disallow remote access unless a compelling business justification exists. • Require management approval of employee remote access. • Regularly review remote access approvals and rescind those that no longer have a compelling business justification. • Restrict remote access to authorized network areas and applications by using VLANs, permissions, and other techniques. • Log remote access communications (including date, time, user, user location, duration, and activity), analyze logs in a timely manner, and follow up on anomalies. • Implement robust authentication methods for remote access. • Use encryption to protect communications between the access device and the institution. • Use application white-listing.42 For institution-owned devices, the institution should have the ability to manage the remote devices. The following controls should be implemented: • Securely configure remote access devices. • Protect remote access devices against malware. • Patch, update, and maintain all software on remote access devices. • Encrypt sensitive data residing on the access device. • Implement secure containers with internal boundaries to store sensitive information, in a way that is not	Functional	Intersects With	Remote Purging	MDM-09	Mechanisms exist to remotely purge selected information from mobile devices.	3		MDM-05

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.15.d	N/A	Management may choose to allow employees to connect remotely to the institution's network using either an institution-owned or a personally owned device (often referred to as BYOD or "bring your own device"). Institution-owned devices are easier to secure because the institution controls the devices' configuration and often can implement remote wiping if the devices are lost or stolen. It may be more difficult to implement remote wiping or a similar measure on an employee's personally owned device. BYOD is becoming more popular, however, with institutions and employees because it reduces costs to the institution and enables employees to carry one device instead of two. For all remote devices, management should do the following to control employee remote access to the institution's network: • Disallow remote access unless a compelling business justification exists. • Require management approval of employee remote access. • Regularly review remote access approvals and rescind those that no longer have a compelling business justification. • Restrict remote access to authorized network areas and applications by using VLANs, permissions, and other techniques. • Log remote access communications (including date, time, user, user location, duration, and activity), analyze logs in a timely manner, and follow up on anomalies. • Implement robust authentication methods for remote access. • Use encryption to protect communications between the access device and the institution. • Use application white-listing.42 For institution-owned devices, the institution should have the ability to manage the remote devices. The following controls should be implemented: • Securely configure remote access devices. • Protect remote access devices against malware. • Patch, update, and maintain all software on remote access devices. • Encrypt sensitive data residing on the access device. • Implement secure containers with internal boundaries to store sensitive information, in a way that is not	Functional	Intersects With	Remote Access Endpoint Security Validation	NET-26.3	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions and patch levels) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	5		NET-14.7
II.C.15.d	N/A	Management may choose to allow employees to connect remotely to the institution's network using either an institution-owned or a personally owned device (often referred to as BYOD or "bring your own device"). Institution-owned devices are easier to secure because the institution controls the devices' configuration and often can implement remote wiping if the devices are lost or stolen. It may be more difficult to implement remote wiping or a similar measure on an employee's personally owned device. BYOD is becoming more popular, however, with institutions and employees because it reduces costs to the institution and enables employees to carry one device instead of two. For all remote devices, management should do the following to control employee remote access to the institution's network: • Disallow remote access unless a compelling business justification exists. • Require management approval of employee remote access. • Regularly review remote access approvals and rescind those that no longer have a compelling business justification. • Restrict remote access to authorized network areas and applications by using VLANs, permissions, and other techniques. • Log remote access communications (including date, time, user, user location, duration, and activity), analyze logs in a timely manner, and follow up on anomalies. • Implement robust authentication methods for remote access. • Use encryption to protect communications between the access device and the institution. • Use application white-listing.42 For institution-owned devices, the institution should have the ability to manage the remote devices. The following controls should be implemented: • Securely configure remote access devices. • Protect remote access devices against malware. • Patch, update, and maintain all software on remote access devices. • Encrypt sensitive data residing on the access device. • Implement secure containers with internal boundaries to store sensitive information, in a way that is not	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-27	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5		NET-14.5
II.C.16	Employee Awareness and Training	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.C.16.a	N/A	The institution's customer awareness and education efforts should consider both retail and commercial account holders and include the following elements: • An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts accessible online. 47 An upstream ISP is usually a large ISP that provides Internet access to a local ISP. 48 See the IT Handbook's "Retail Payment Systems" booklet, appendix E, "Mobile Financial Services." • An explanation that while the institution may contact a customer regarding his or her account or suspicious activities related to his or her account, the institution should never ask the customer to provide his or her log-in credentials over the phone or via e-mail. • A list of recommended controls and prudent practices that the customer should implement when using the institution's remote financial services. • A suggestion that commercial online customers perform a related risk assessment and controls evaluation periodically. • Recommendations of technical and business controls to commercial customers that can be implemented to mitigate the risks from fraud schemes such as Business Email Compromise.49 • A method to contact the institution if	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	3		IRO-11
II.C.17	N/A	Application Security Action Summary Management should use applications that have been developed following secure development practices and that meet a prudent level of security. Management should develop security control requirements for all applications, whether the institution acquires or develops them. Information security personnel should be involved in monitoring the application development process to verify that secure development practices are followed, security controls are implemented, and information security needs are met. Institutions and their customers use a wide variety of applications. Such applications include core banking applications, web applications, and installable applications (e.g., downloadable mobile applications). A secure software development life cycle ensures that Internet- and client-facing applications have the necessary security controls. The institution should ensure that all applications are securely developed. To verify the controls have been developed and implemented appropriately, management should perform appropriate tests (e.g., penetration tests, vulnerability assessments, and application security tests) before launching or making significant changes to external-facing applications. Issues noted from tests should be remediated before launching applications or moving changes into production. At institutions that employ third parties to develop applications, management should ensure that the third parties meet the same controls. Applications should provide the ability for management to do the following: • Implement a prudent set of security controls (e.g., password and audit policies), audit trails of security and access changes, and user activity logs for all applications. • Establish user and group profiles for applications if not part of a centralized identity access management system. 49 See Federal Bureau of Investigation, Alert I-012215-PSA. • Change and disable default application accounts upon installation. • Review and install	Functional	Intersects With	Web Application Firewall (WAF)	NET-34	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	3		WEB-03

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.17	N/A	Application Security Action Summary Management should use applications that have been developed following secure development practices and that meet a prudent level of security. Management should develop security control requirements for all applications, whether the institution acquires or develops them. Information security personnel should be involved in monitoring the application development process to verify that secure development practices are followed, security controls are implemented, and information security needs are met. Institutions and their customers use a wide variety of applications. Such applications include core banking applications, web applications, and installable applications (e.g., downloadable mobile applications). A secure software development life cycle ensures that Internet- and client-facing applications have the necessary security controls. The institution should ensure that all applications are securely developed. To verify the controls have been developed and implemented appropriately, management should perform appropriate tests (e.g., penetration tests, vulnerability assessments, and application security tests) before launching or making significant changes to external-facing applications. Issues noted from tests should be remediated before launching applications or moving changes into production. At institutions that employ third parties to develop applications, management should ensure that the third parties meet the same controls. Applications should provide the ability for management to do the following: • Implement a prudent set of security controls (e.g., password and audit policies), audit trails of security and access changes, and user activity logs for all applications. • Establish user and group profiles for applications if not part of a centralized identity access management system. 49 See Federal Bureau of Investigation, Alert I-012215-PSA. • Change and disable default application accounts upon installation. • Review and install	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-09	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5		PRM-05
II.C.17	N/A	Application Security Action Summary Management should use applications that have been developed following secure development practices and that meet a prudent level of security. Management should develop security control requirements for all applications, whether the institution acquires or develops them. Information security personnel should be involved in monitoring the application development process to verify that secure development practices are followed, security controls are implemented, and information security needs are met. Institutions and their customers use a wide variety of applications. Such applications include core banking applications, web applications, and installable applications (e.g., downloadable mobile applications). A secure software development life cycle ensures that Internet- and client-facing applications have the necessary security controls. The institution should ensure that all applications are securely developed. To verify the controls have been developed and implemented appropriately, management should perform appropriate tests (e.g., penetration tests, vulnerability assessments, and application security tests) before launching or making significant changes to external-facing applications. Issues noted from tests should be remediated before launching applications or moving changes into production. At institutions that employ third parties to develop applications, management should ensure that the third parties meet the same controls. Applications should provide the ability for management to do the following: • Implement a prudent set of security controls (e.g., password and audit policies), audit trails of security and access changes, and user activity logs for all applications. • Establish user and group profiles for applications if not part of a centralized identity access management system. 49 See Federal Bureau of Investigation, Alert I-012215-PSA. • Change and disable default application accounts upon installation. • Review and install	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8		TDA-06
II.C.17	N/A	Application Security Action Summary Management should use applications that have been developed following secure development practices and that meet a prudent level of security. Management should develop security control requirements for all applications, whether the institution acquires or develops them. Information security personnel should be involved in monitoring the application development process to verify that secure development practices are followed, security controls are implemented, and information security needs are met. Institutions and their customers use a wide variety of applications. Such applications include core banking applications, web applications, and installable applications (e.g., downloadable mobile applications). A secure software development life cycle ensures that Internet- and client-facing applications have the necessary security controls. The institution should ensure that all applications are securely developed. To verify the controls have been developed and implemented appropriately, management should perform appropriate tests (e.g., penetration tests, vulnerability assessments, and application security tests) before launching or making significant changes to external-facing applications. Issues noted from tests should be remediated before launching applications or moving changes into production. At institutions that employ third parties to develop applications, management should ensure that the third parties meet the same controls. Applications should provide the ability for management to do the following: • Implement a prudent set of security controls (e.g., password and audit policies), audit trails of security and access changes, and user activity logs for all applications. • Establish user and group profiles for applications if not part of a centralized identity access management system. 49 See Federal Bureau of Investigation, Alert I-012215-PSA. • Change and disable default application accounts upon installation. • Review and install	Functional	Intersects With	Input Data Validation	TDA-12	Mechanisms exist to check the validity of information inputs.	3		TDA-18

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL:	https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL:	https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.17	N/A	Application Security Action Summary Management should use applications that have been developed following secure development practices and that meet a prudent level of security. Management should develop security control requirements for all applications, whether the institution acquires or develops them. Information security personnel should be involved in monitoring the application development process to verify that secure development practices are followed, security controls are implemented, and information security needs are met. Institutions and their customers use a wide variety of applications. Such applications include core banking applications, web applications, and installable applications (e.g., downloadable mobile applications). A secure software development life cycle ensures that Internet- and client-facing applications have the necessary security controls. The institution should ensure that all applications are securely developed. To verify the controls have been developed and implemented appropriately, management should perform appropriate tests (e.g., penetration tests, vulnerability assessments, and application security tests) before launching or making significant changes to external-facing applications. Issues noted from tests should be remediated before launching applications or moving changes into production. At institutions that employ third parties to develop applications, management should ensure that the third parties meet the same controls. Applications should provide the ability for management to do the following: • Implement a prudent set of security controls (e.g., password and audit policies), audit trails of security and access changes, and user activity logs for all applications. • Establish user and group profiles for applications if not part of a centralized identity access management system. 49 See Federal Bureau of Investigation, Alert I-012215-PSA. • Change and disable default application accounts upon installation. • Review and install	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.	5		TDA-09
II.C.18	N/A	Database Security Action Summary Management should implement effective controls for databases and restrict access appropriately. Databases are collections of information organized to be easily accessed, managed, and updated. Databases can be developed in-house or purchased from third parties and have their own controls and protective mechanisms configured to provide varying levels of protection. Along with many other security features, encryption helps to protect the stored information from theft or unauthorized viewing. Management should implement or enable controls commensurate with the sensitivity of the data stored in or accessed by the database. Database users may be people (e.g., employees, customers, and contractors) or other applications. Users have different levels of access and authorization. Some users may have extensive privileges, including the ability to change the database configuration and access controls. Other users may have restrictions in what they can view, manipulate, or store. When a person is the database user, authorizations can be tailored to that person, greatly limiting the amount of information that could be exposed in a security incident. When an application is the database user, the access granted to the application can be more extensive than a person would require. Accordingly, an attack on a database through an application could expose a larger and more damaging collection of data. For application accounts, management should strengthen authentication and monitoring requirements to minimize the potential for unauthorized use. Management should appropriately control user access and apply the principle of least privilege in assigning authorizations. The use and overall configuration of a database's security features should be part of a well-designed, layered security program.	Functional	Intersects With	Database Encryption	CRY-08	Mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.	5		CRY-05.3
II.C.18	N/A	Database Security Action Summary Management should implement effective controls for databases and restrict access appropriately. Databases are collections of information organized to be easily accessed, managed, and updated. Databases can be developed in-house or purchased from third parties and have their own controls and protective mechanisms configured to provide varying levels of protection. Along with many other security features, encryption helps to protect the stored information from theft or unauthorized viewing. Management should implement or enable controls commensurate with the sensitivity of the data stored in or accessed by the database. Database users may be people (e.g., employees, customers, and contractors) or other applications. Users have different levels of access and authorization. Some users may have extensive privileges, including the ability to change the database configuration and access controls. Other users may have restrictions in what they can view, manipulate, or store. When a person is the database user, authorizations can be tailored to that person, greatly limiting the amount of information that could be exposed in a security incident. When an application is the database user, the access granted to the application can be more extensive than a person would require. Accordingly, an attack on a database through an application could expose a larger and more damaging collection of data. For application accounts, management should strengthen authentication and monitoring requirements to minimize the potential for unauthorized use. Management should appropriately control user access and apply the principle of least privilege in assigning authorizations. The use and overall configuration of a database's security features should be part of a well-designed, layered security program.	Functional	Intersects With	Database Access	IAC-25.2	Mechanisms exist to restrict access to databases containing sensitive and/or regulated data to only necessary Technology Assets, Applications and/or Services (TAAS) or those individuals whose job requires such access.	8		IAC-20.2
II.C.18	N/A	Database Security Action Summary Management should implement effective controls for databases and restrict access appropriately. Databases are collections of information organized to be easily accessed, managed, and updated. Databases can be developed in-house or purchased from third parties and have their own controls and protective mechanisms configured to provide varying levels of protection. Along with many other security features, encryption helps to protect the stored information from theft or unauthorized viewing. Management should implement or enable controls commensurate with the sensitivity of the data stored in or accessed by the database. Database users may be people (e.g., employees, customers, and contractors) or other applications. Users have different levels of access and authorization. Some users may have extensive privileges, including the ability to change the database configuration and access controls. Other users may have restrictions in what they can view, manipulate, or store. When a person is the database user, authorizations can be tailored to that person, greatly limiting the amount of information that could be exposed in a security incident. When an application is the database user, the access granted to the application can be more extensive than a person would require. Accordingly, an attack on a database through an application could expose a larger and more damaging collection of data. For application accounts, management should strengthen authentication and monitoring requirements to minimize the potential for unauthorized use. Management should appropriately control user access and apply the principle of least privilege in assigning authorizations. The use and overall configuration of a database's security features should be part of a well-designed, layered security program.	Functional	Intersects With	Database Logging	MON-32	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	5		MON-03.7

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL:	https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL:	https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.18	N/A	Database Security Action Summary Management should implement effective controls for databases and restrict access appropriately. Databases are collections of information organized to be easily accessed, managed, and updated. Databases can be developed in-house or purchased from third parties and have their own controls and protective mechanisms configured to provide varying levels of protection. Along with many other security features, encryption helps to protect the stored information from theft or unauthorized viewing. Management should implement or enable controls commensurate with the sensitivity of the data stored in or accessed by the database. Database users may be people (e.g., employees, customers, and contractors) or other applications. Users have different levels of access and authorization. Some users may have extensive privileges, including the ability to change the database configuration and access controls. Other users may have restrictions in what they can view, manipulate, or store. When a person is the database user, authorizations can be tailored to that person, greatly limiting the amount of information that could be exposed in a security incident. When an application is the database user, the access granted to the application can be more extensive than a person would require. Accordingly, an attack on a database through an application could expose a larger and more damaging collection of data. For application accounts, management should strengthen authentication and monitoring requirements to minimize the potential for unauthorized use. Management should appropriately control user access and apply the principle of least privilege in assigning authorizations. The use and overall configuration of a database's security features should be part of a well-designed, layered security program.	Functional	Intersects With	Database Administrative Processes	OPS-04.2	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.	5		AST-28
II.C.19	N/A	Encryption Action Summary Management should implement the type and level of encryption commensurate with the sensitivity of the information. 52 Resources include software tools, industry resources, specific certifications, and education courses. Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. Encryption can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols. Encryption can be used as a preventive control, a detective control, or both. As a preventive control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow management to discover unauthorized changes to data. When prevention and detection are joined, encryption can be an important control in ensuring confidentiality, integrity, and availability. Institution management should employ encryption strength sufficient to protect information from disclosure. Encryption methods should be reviewed periodically to ensure that the types and methods of encryption are still secure as technology and threats evolve. Decisions regarding what data to encrypt and at what points to encrypt the data are typically based on the risk of disclosure and the costs of encryption. The need to encrypt data is determined by the institution's data classification and risk assessment. Passwords should be hashed or encrypted in storage. Passwords that are hashed also should be salted.53 Files containing encrypted or hashed passwords used by systems to authenticate users should be readable only with elevated (or administrator) privileges. Key management54 is crucial to the effective use of encryption. Effective key management systems rely on an agreed set of standards, procedures, and secure methods that address the following:55 • Generating keys for different cryptographic	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8		CRY-01
II.C.19	N/A	Encryption Action Summary Management should implement the type and level of encryption commensurate with the sensitivity of the information. 52 Resources include software tools, industry resources, specific certifications, and education courses. Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. Encryption can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols. Encryption can be used as a preventive control, a detective control, or both. As a preventive control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow management to discover unauthorized changes to data. When prevention and detection are joined, encryption can be an important control in ensuring confidentiality, integrity, and availability. Institution management should employ encryption strength sufficient to protect information from disclosure. Encryption methods should be reviewed periodically to ensure that the types and methods of encryption are still secure as technology and threats evolve. Decisions regarding what data to encrypt and at what points to encrypt the data are typically based on the risk of disclosure and the costs of encryption. The need to encrypt data is determined by the institution's data classification and risk assessment. Passwords should be hashed or encrypted in storage. Passwords that are hashed also should be salted.53 Files containing encrypted or hashed passwords used by systems to authenticate users should be readable only with elevated (or administrator) privileges. Key management54 is crucial to the effective use of encryption. Effective key management systems rely on an agreed set of standards, procedures, and secure methods that address the following:55 • Generating keys for different cryptographic	Functional	Intersects With	Cryptographic Cipher Suites and Protocols Inventory	CRY-04	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.	3		CRY-01.5
II.C.19	N/A	Encryption Action Summary Management should implement the type and level of encryption commensurate with the sensitivity of the information. 52 Resources include software tools, industry resources, specific certifications, and education courses. Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. Encryption can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols. Encryption can be used as a preventive control, a detective control, or both. As a preventive control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow management to discover unauthorized changes to data. When prevention and detection are joined, encryption can be an important control in ensuring confidentiality, integrity, and availability. Institution management should employ encryption strength sufficient to protect information from disclosure. Encryption methods should be reviewed periodically to ensure that the types and methods of encryption are still secure as technology and threats evolve. Decisions regarding what data to encrypt and at what points to encrypt the data are typically based on the risk of disclosure and the costs of encryption. The need to encrypt data is determined by the institution's data classification and risk assessment. Passwords should be hashed or encrypted in storage. Passwords that are hashed also should be salted.53 Files containing encrypted or hashed passwords used by systems to authenticate users should be readable only with elevated (or administrator) privileges. Key management54 is crucial to the effective use of encryption. Effective key management systems rely on an agreed set of standards, procedures, and secure methods that address the following:55 • Generating keys for different cryptographic	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.19	N/A	Encryption Action Summary Management should implement the type and level of encryption commensurate with the sensitivity of the information. 52 Resources include software tools, industry resources, specific certifications, and education courses. Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. Encryption can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols. Encryption can be used as a preventive control, a detective control, or both. As a preventive control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow management to discover unauthorized changes to data. When prevention and detection are joined, encryption can be an important control in ensuring confidentiality, integrity, and availability. Institution management should employ encryption strength sufficient to protect information from disclosure. Encryption methods should be reviewed periodically to ensure that the types and methods of encryption are still secure as technology and threats evolve. Decisions regarding what data to encrypt and at what points to encrypt the data are typically based on the risk of disclosure and the costs of encryption. The need to encrypt data is determined by the institution's data classification and risk assessment. Passwords should be hashed or encrypted in storage. Passwords that are hashed also should be salted.53 Files containing encrypted or hashed passwords used by systems to authenticate users should be readable only with elevated (or administrator) privileges. Key management54 is crucial to the effective use of encryption. Effective key management systems rely on an agreed set of standards, procedures, and secure methods that address the following:55 • Generating keys for different cryptographic	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	5		CRY-05
II.C.19	N/A	Encryption Action Summary Management should implement the type and level of encryption commensurate with the sensitivity of the information. 52 Resources include software tools, industry resources, specific certifications, and education courses. Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information. Encryption can be used throughout a technological environment, including the operating systems, middleware, applications, file systems, and communications protocols. Encryption can be used as a preventive control, a detective control, or both. As a preventive control, encryption acts to protect data from disclosure to unauthorized parties. As a detective control, encryption is used to allow management to discover unauthorized changes to data. When prevention and detection are joined, encryption can be an important control in ensuring confidentiality, integrity, and availability. Institution management should employ encryption strength sufficient to protect information from disclosure. Encryption methods should be reviewed periodically to ensure that the types and methods of encryption are still secure as technology and threats evolve. Decisions regarding what data to encrypt and at what points to encrypt the data are typically based on the risk of disclosure and the costs of encryption. The need to encrypt data is determined by the institution's data classification and risk assessment. Passwords should be hashed or encrypted in storage. Passwords that are hashed also should be salted.53 Files containing encrypted or hashed passwords used by systems to authenticate users should be readable only with elevated (or administrator) privileges. Key management54 is crucial to the effective use of encryption. Effective key management systems rely on an agreed set of standards, procedures, and secure methods that address the following:55 • Generating keys for different cryptographic	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	8		CRY-09
II.C.20	Third-Party Service Providers	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.C.20.a	N/A	As with other forms of outsourcing, information security implications are key in the cloud computing model. Management may need to revise information security policies, standards, and procedures to incorporate the activities related to a cloud computing service provider. Refer to the FFIEC's "Outsourced Cloud Computing" statement for more information.56	Functional	Intersects With	Cloud Services	CLD-02	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5		CLD-01
II.C.20.a	N/A	As with other forms of outsourcing, information security implications are key in the cloud computing model. Management may need to revise information security policies, standards, and procedures to incorporate the activities related to a cloud computing service provider. Refer to the FFIEC's "Outsourced Cloud Computing" statement for more information.56	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-04
II.C.20.b	N/A	Management may rely on third parties to provide security services; management, however, remains responsible for ensuring the security of the institution's systems and information by overseeing the effectiveness of the services provided by the managed security services provider. Additional information is available in appendix D of the IT Handbook's "Outsourcing Technology Services" booklet.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04
II.C.20.b	N/A	Management may rely on third parties to provide security services; management, however, remains responsible for ensuring the security of the institution's systems and information by overseeing the effectiveness of the services provided by the managed security services provider. Additional information is available in appendix D of the IT Handbook's "Outsourcing Technology Services" booklet.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
II.C.21	N/A	Business Continuity Considerations Action Summary Management should do the following: • Identify personnel who will have critical information security roles during a disaster, and train personnel in those roles. • Define information security needs for backup sites and alternate communication networks. • Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios. Business continuity plans should be reviewed as an integral part of the security process. Strategies should consider the different risk environments and the degree of risk mitigation necessary to protect the institution if continuity plans must be implemented. Management should train personnel regarding their security roles during a disaster. Additionally, management should update technologies and plans for backup sites and communications networks. These security considerations should be integrated with the testing of the business continuity plan. Information security events may trigger activation of the business continuity plan. Therefore, the institution's plan should include steps that explicitly address information security incident response and resilience. Resilience testing should incorporate information security event scenarios identified by the institution. Refer to the IT Handbook's "Business Continuity Planning" booklet for more information. 56 See FFIEC, "Outsourced Cloud Computing," July 10,	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	5		BCD-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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.21	N/A	Business Continuity Considerations Action Summary Management should do the following: • Identify personnel who will have critical information security roles during a disaster, and train personnel in those roles. • Define information security needs for backup sites and alternate communication networks. • Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios. Business continuity plans should be reviewed as an integral part of the security process. Strategies should consider the different risk environments and the degree of risk mitigation necessary to protect the institution if continuity plans must be implemented. Management should train personnel regarding their security roles during a disaster. Additionally, management should update technologies and plans for backup sites and communications networks. These security considerations should be integrated with the testing of the business continuity plan. Information security events may trigger activation of the business continuity plan. Therefore, the institution's plan should include steps that explicitly address information security incident response and resilience. Resilience testing should incorporate information security event scenarios identified by the institution. Refer to the IT Handbook's "Business Continuity Planning" booklet for more information. 56 See FFIEC, "Outsourced Cloud Computing," July 10,	Functional	Intersects With	Contingency Training	BCD-09	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	5		BCD-03
II.C.21	N/A	Business Continuity Considerations Action Summary Management should do the following: • Identify personnel who will have critical information security roles during a disaster, and train personnel in those roles. • Define information security needs for backup sites and alternate communication networks. • Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios. Business continuity plans should be reviewed as an integral part of the security process. Strategies should consider the different risk environments and the degree of risk mitigation necessary to protect the institution if continuity plans must be implemented. Management should train personnel regarding their security roles during a disaster. Additionally, management should update technologies and plans for backup sites and communications networks. These security considerations should be integrated with the testing of the business continuity plan. Information security events may trigger activation of the business continuity plan. Therefore, the institution's plan should include steps that explicitly address information security incident response and resilience. Resilience testing should incorporate information security event scenarios identified by the institution. Refer to the IT Handbook's "Business Continuity Planning" booklet for more information. 56 See FFIEC, "Outsourced Cloud Computing," July 10,	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
II.C.21	N/A	Business Continuity Considerations Action Summary Management should do the following: • Identify personnel who will have critical information security roles during a disaster, and train personnel in those roles. • Define information security needs for backup sites and alternate communication networks. • Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios. Business continuity plans should be reviewed as an integral part of the security process. Strategies should consider the different risk environments and the degree of risk mitigation necessary to protect the institution if continuity plans must be implemented. Management should train personnel regarding their security roles during a disaster. Additionally, management should update technologies and plans for backup sites and communications networks. These security considerations should be integrated with the testing of the business continuity plan. Information security events may trigger activation of the business continuity plan. Therefore, the institution's plan should include steps that explicitly address information security incident response and resilience. Resilience testing should incorporate information security event scenarios identified by the institution. Refer to the IT Handbook's "Business Continuity Planning" booklet for more information. 56 See FFIEC, "Outsourced Cloud Computing," July 10,	Functional	Intersects With	Alternate Processing Site	BCD-13	Mechanisms exist to establish an alternate processing site that provides processing capability and security measures equivalent to that of the primary site.	5		BCD-09
II.C.21	N/A	Business Continuity Considerations Action Summary Management should do the following: • Identify personnel who will have critical information security roles during a disaster, and train personnel in those roles. • Define information security needs for backup sites and alternate communication networks. • Establish and maintain policies that address the concepts of information security incident response and resilience, and test information security incident scenarios. Business continuity plans should be reviewed as an integral part of the security process. Strategies should consider the different risk environments and the degree of risk mitigation necessary to protect the institution if continuity plans must be implemented. Management should train personnel regarding their security roles during a disaster. Additionally, management should update technologies and plans for backup sites and communications networks. These security considerations should be integrated with the testing of the business continuity plan. Information security events may trigger activation of the business continuity plan. Therefore, the institution's plan should include steps that explicitly address information security incident response and resilience. Resilience testing should incorporate information security event scenarios identified by the institution. Refer to the IT Handbook's "Business Continuity Planning" booklet for more information. 56 See FFIEC, "Outsourced Cloud Computing," July 10,	Functional	Intersects With	Incident Response Capabilities Testing Coordination with Related Plans	IRO-09.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	3		IRO-06.1
II.C.22	N/A	Log Management Network and host activities typically are recorded on the host and sent across the network to a central logging repository. The data that arrive at the repository are in the format of the software that recorded the activity. The logging repository may process the data and can enable timely and effective log analysis. Management should have effective log retention policies that address the significance of maintaining logs for incident response and analysis needs. Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Intruders often attempt to conceal unauthorized access by editing or deleting log files. Therefore, institutions should strictly control and monitor access to log files whether on the host or in a centralized logging repository. Considerations for securing the integrity of log files include the following: • Encrypting log files that contain sensitive data or that are transmitted over the network. • Ensuring adequate storage capacity to avoid gaps in data gathering. • Securing backup and disposal of log files. • Logging the data to a separate, isolated computer. • Logging the data to read-only media. • Setting logging parameters to disallow any modification to previously written data. • Restricting access to log files to a limited number of authorized users. Additionally, logging practices should be reviewed periodically by an independent party to ensure appropriate log management. Logs are voluminous and challenging to read. They come from a variety of systems and can be difficult to manage and correlate. Security information and event management (SIEM) systems can provide a method for management to collect, aggregate, analyze, and correlate information from discrete systems and applications. Management can use SIEM systems to discern trends and identify potential information security incidents. SIEM systems can be used to gather information from the following: • Network and security devices and systems.57 • Identity and access management	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

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.22	N/A	Log Management Network and host activities typically are recorded on the host and sent across the network to a central logging repository. The data that arrive at the repository are in the format of the software that recorded the activity. The logging repository may process the data and can enable timely and effective log analysis. Management should have effective log retention policies that address the significance of maintaining logs for incident response and analysis needs. Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Intruders often attempt to conceal unauthorized access by editing or deleting log files. Therefore, institutions should strictly control and monitor access to log files whether on the host or in a centralized logging repository. Considerations for securing the integrity of log files include the following: • Encrypting log files that contain sensitive data or that are transmitted over the network. • Ensuring adequate storage capacity to avoid gaps in data gathering. • Securing backup and disposal of log files. • Logging the data to a separate, isolated computer. • Logging the data to read-only media. • Setting logging parameters to disallow any modification to previously written data. • Restricting access to log files to a limited number of authorized users. Additionally, logging practices should be reviewed periodically by an independent party to ensure appropriate log management. Logs are voluminous and challenging to read. They come from a variety of systems and can be difficult to manage and correlate. Security information and event management (SIEM) systems can provide a method for management to collect, aggregate, analyze, and correlate information from discrete systems and applications. Management can use SIEM systems to discern trends and identify potential information security incidents. SIEM systems can be used to gather information from the following: • Network and security devices and systems.57 • Identity and access management	Functional	Intersects With	Correlate Monitoring Information	MON-08	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		MON-02.1
II.C.22	N/A	Log Management Network and host activities typically are recorded on the host and sent across the network to a central logging repository. The data that arrive at the repository are in the format of the software that recorded the activity. The logging repository may process the data and can enable timely and effective log analysis. Management should have effective log retention policies that address the significance of maintaining logs for incident response and analysis needs. Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Intruders often attempt to conceal unauthorized access by editing or deleting log files. Therefore, institutions should strictly control and monitor access to log files whether on the host or in a centralized logging repository. Considerations for securing the integrity of log files include the following: • Encrypting log files that contain sensitive data or that are transmitted over the network. • Ensuring adequate storage capacity to avoid gaps in data gathering. • Securing backup and disposal of log files. • Logging the data to a separate, isolated computer. • Logging the data to read-only media. • Setting logging parameters to disallow any modification to previously written data. • Restricting access to log files to a limited number of authorized users. Additionally, logging practices should be reviewed periodically by an independent party to ensure appropriate log management. Logs are voluminous and challenging to read. They come from a variety of systems and can be difficult to manage and correlate. Security information and event management (SIEM) systems can provide a method for management to collect, aggregate, analyze, and correlate information from discrete systems and applications. Management can use SIEM systems to discern trends and identify potential information security incidents. SIEM systems can be used to gather information from the following: • Network and security devices and systems.57 • Identity and access management	Functional	Intersects With	Event Log & Security-Relevant Telemetry Storage Capacity	MON-10	Mechanisms exist to allocate and proactively manage sufficient event log and security-relevant telemetry storage capacity to reduce the likelihood of such capacity being exceeded.	3		MON-04
II.C.22	N/A	Log Management Network and host activities typically are recorded on the host and sent across the network to a central logging repository. The data that arrive at the repository are in the format of the software that recorded the activity. The logging repository may process the data and can enable timely and effective log analysis. Management should have effective log retention policies that address the significance of maintaining logs for incident response and analysis needs. Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Intruders often attempt to conceal unauthorized access by editing or deleting log files. Therefore, institutions should strictly control and monitor access to log files whether on the host or in a centralized logging repository. Considerations for securing the integrity of log files include the following: • Encrypting log files that contain sensitive data or that are transmitted over the network. • Ensuring adequate storage capacity to avoid gaps in data gathering. • Securing backup and disposal of log files. • Logging the data to a separate, isolated computer. • Logging the data to read-only media. • Setting logging parameters to disallow any modification to previously written data. • Restricting access to log files to a limited number of authorized users. Additionally, logging practices should be reviewed periodically by an independent party to ensure appropriate log management. Logs are voluminous and challenging to read. They come from a variety of systems and can be difficult to manage and correlate. Security information and event management (SIEM) systems can provide a method for management to collect, aggregate, analyze, and correlate information from discrete systems and applications. Management can use SIEM systems to discern trends and identify potential information security incidents. SIEM systems can be used to gather information from the following: • Network and security devices and systems.57 • Identity and access management	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
II.C.22	N/A	Log Management Network and host activities typically are recorded on the host and sent across the network to a central logging repository. The data that arrive at the repository are in the format of the software that recorded the activity. The logging repository may process the data and can enable timely and effective log analysis. Management should have effective log retention policies that address the significance of maintaining logs for incident response and analysis needs. Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Intruders often attempt to conceal unauthorized access by editing or deleting log files. Therefore, institutions should strictly control and monitor access to log files whether on the host or in a centralized logging repository. Considerations for securing the integrity of log files include the following: • Encrypting log files that contain sensitive data or that are transmitted over the network. • Ensuring adequate storage capacity to avoid gaps in data gathering. • Securing backup and disposal of log files. • Logging the data to a separate, isolated computer. • Logging the data to read-only media. • Setting logging parameters to disallow any modification to previously written data. • Restricting access to log files to a limited number of authorized users. Additionally, logging practices should be reviewed periodically by an independent party to ensure appropriate log management. Logs are voluminous and challenging to read. They come from a variety of systems and can be difficult to manage and correlate. Security information and event management (SIEM) systems can provide a method for management to collect, aggregate, analyze, and correlate information from discrete systems and applications. Management can use SIEM systems to discern trends and identify potential information security incidents. SIEM systems can be used to gather information from the following: • Network and security devices and systems.57 • Identity and access management	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5		MON-10
II.D	Security Operations	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
II.D.1	N/A	Metrics A mature and effective information security program uses metrics to improve the program's effectiveness and efficiency. Management should develop metrics that demonstrate the extent to which the security program is implemented and whether the program is effective. Metrics are used to measure security policy implementation, conformance with the information security program, the adequacy of security services delivery, and the impact of security events on business processes. The measurement of security characteristics can allow management to increase control and drive improvements to the security process. Metrics generally are formed to measure conformance to the standards and procedures that are used to implement policies. Management should utilize metrics to quantify and report risks of the information security program. Metrics should be gathered from external sources and internal data. The scope of metrics should be comprehensive and commensurate with the complexity of the institution's operations. Reports should incorporate metrics tailored for different audiences and stakeholders. These metrics and other monitoring reports of the information security program should feed into ITRM reporting.	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	8		GOV-05
II.D.1	N/A	Metrics A mature and effective information security program uses metrics to improve the program's effectiveness and efficiency. Management should develop metrics that demonstrate the extent to which the security program is implemented and whether the program is effective. Metrics are used to measure security policy implementation, conformance with the information security program, the adequacy of security services delivery, and the impact of security events on business processes. The measurement of security characteristics can allow management to increase control and drive improvements to the security process. Metrics generally are formed to measure conformance to the standards and procedures that are used to implement policies. Management should utilize metrics to quantify and report risks of the information security program. Metrics should be gathered from external sources and internal data. The scope of metrics should be comprehensive and commensurate with the complexity of the institution's operations. Reports should incorporate metrics tailored for different audiences and stakeholders. These metrics and other monitoring reports of the information security program should feed into ITRM reporting.	Functional	Intersects With	Key Performance Indicators (KPIs)	GOV-12.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring, trend analysis, and possible control redesign or replacement for the Security, Compliance & Resilience Program (SCRP).	5		GOV-05.1
II.D.1	N/A	Metrics A mature and effective information security program uses metrics to improve the program's effectiveness and efficiency. Management should develop metrics that demonstrate the extent to which the security program is implemented and whether the program is effective. Metrics are used to measure security policy implementation, conformance with the information security program, the adequacy of security services delivery, and the impact of security events on business processes. The measurement of security characteristics can allow management to increase control and drive improvements to the security process. Metrics generally are formed to measure conformance to the standards and procedures that are used to implement policies. Management should utilize metrics to quantify and report risks of the information security program. Metrics should be gathered from external sources and internal data. The scope of metrics should be comprehensive and commensurate with the complexity of the institution's operations. Reports should incorporate metrics tailored for different audiences and stakeholders. These metrics and other monitoring reports of the information security program should feed into ITRM reporting.	Functional	Intersects With	Key Risk Indicators (KRIs)	GOV-12.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring, trend analysis, and possible control redesign or replacement for the Security, Compliance & Resilience Program (SCRP).	5		GOV-05.2
III	Conclusion	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
III.A	N/A	Threat Identification and Assessment Action Summary Management should do the following: • Identify and assess threats. • Use threat knowledge to drive risk assessment and response. • Design policies to allow immediate and consequential threats to be dealt with expeditiously. Threat identification and assessment involves discovering knowledge about threat sources and vulnerabilities and analyzing the potential for exploitation. This is much more focused than the risk identification process described in the "Risk Identification" section of this booklet. Information gained from threat identification and assessment should be used in risk assessment and response to drive protective and detective strategies and tactics. Strategies involve the information security program's policies, standards, and procedures, and the implementing technologies. Examples of tactics include threat signatures used for incident identification and management of threat behaviors. NIST notes that types of threat sources include the following: • Hostile cyber or physical attacks. • Human errors of omission or commission. • Structural failures of organization-controlled resources (e.g., hardware, software, and environmental controls). • Natural and man-made disasters, accidents, and failures beyond the control of the organization.59 Management should develop procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information. The identification of threats involves the sources of threats, their capabilities, and their objectives. Information about threats generally comes from government (e.g., US-CERT), information-sharing organizations (e.g., FS-ISAC), industry sources, the institution, and third parties. Third-party information may be from organizations that specifically track and report on threats or from third-party reports of past activity. Some of those 59 NIST SP 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments,"	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.	8		THR-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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
III.A	N/A	Threat Identification and Assessment Action Summary Management should do the following: • Identify and assess threats. • Use threat knowledge to drive risk assessment and response. • Design policies to allow immediate and consequential threats to be dealt with expeditiously. Threat identification and assessment involves discovering knowledge about threat sources and vulnerabilities and analyzing the potential for exploitation. This is much more focused than the risk identification process described in the "Risk Identification" section of this booklet. Information gained from threat identification and assessment should be used in risk assessment and response to drive protective and detective strategies and tactics. Strategies involve the information security program's policies, standards, and procedures, and the implementing technologies. Examples of tactics include threat signatures used for incident identification and management of threat behaviors. NIST notes that types of threat sources include the following: • Hostile cyber or physical attacks. • Human errors of omission or commission. • Structural failures of organization-controlled resources (e.g., hardware, software, and environmental controls). • Natural and man-made disasters, accidents, and failures beyond the control of the organization.59 Management should develop procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information. The identification of threats involves the sources of threats, their capabilities, and their objectives. Information about threats generally comes from government (e.g., US-CERT), information-sharing organizations (e.g., FS-ISAC), industry sources, the institution, and third parties. Third-party information may be from organizations that specifically track and report on threats or from third-party reports of past activity. Some of those 59 NIST SP 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments,"	Functional	Intersects With	Threat Intelligence Feeds	THR-04	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5		THR-03
III.A	N/A	Threat Identification and Assessment Action Summary Management should do the following: • Identify and assess threats. • Use threat knowledge to drive risk assessment and response. • Design policies to allow immediate and consequential threats to be dealt with expeditiously. Threat identification and assessment involves discovering knowledge about threat sources and vulnerabilities and analyzing the potential for exploitation. This is much more focused than the risk identification process described in the "Risk Identification" section of this booklet. Information gained from threat identification and assessment should be used in risk assessment and response to drive protective and detective strategies and tactics. Strategies involve the information security program's policies, standards, and procedures, and the implementing technologies. Examples of tactics include threat signatures used for incident identification and management of threat behaviors. NIST notes that types of threat sources include the following: • Hostile cyber or physical attacks. • Human errors of omission or commission. • Structural failures of organization-controlled resources (e.g., hardware, software, and environmental controls). • Natural and man-made disasters, accidents, and failures beyond the control of the organization.59 Management should develop procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information. The identification of threats involves the sources of threats, their capabilities, and their objectives. Information about threats generally comes from government (e.g., US-CERT), information-sharing organizations (e.g., FS-ISAC), industry sources, the institution, and third parties. Third-party information may be from organizations that specifically track and report on threats or from third-party reports of past activity. Some of those 59 NIST SP 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments,"	Functional	Intersects With	Threat Catalog	THR-06	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5		THR-09
III.A	N/A	Threat Identification and Assessment Action Summary Management should do the following: • Identify and assess threats. • Use threat knowledge to drive risk assessment and response. • Design policies to allow immediate and consequential threats to be dealt with expeditiously. Threat identification and assessment involves discovering knowledge about threat sources and vulnerabilities and analyzing the potential for exploitation. This is much more focused than the risk identification process described in the "Risk Identification" section of this booklet. Information gained from threat identification and assessment should be used in risk assessment and response to drive protective and detective strategies and tactics. Strategies involve the information security program's policies, standards, and procedures, and the implementing technologies. Examples of tactics include threat signatures used for incident identification and management of threat behaviors. NIST notes that types of threat sources include the following: • Hostile cyber or physical attacks. • Human errors of omission or commission. • Structural failures of organization-controlled resources (e.g., hardware, software, and environmental controls). • Natural and man-made disasters, accidents, and failures beyond the control of the organization.59 Management should develop procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information. The identification of threats involves the sources of threats, their capabilities, and their objectives. Information about threats generally comes from government (e.g., US-CERT), information-sharing organizations (e.g., FS-ISAC), industry sources, the institution, and third parties. Third-party information may be from organizations that specifically track and report on threats or from third-party reports of past activity. Some of those 59 NIST SP 800-30, revision 1, "Information Security: Guide for Conducting Risk Assessments,"	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5		THR-10
III.B	N/A	Threat Monitoring Threat monitoring policies should provide for continual and ad hoc monitoring of threat intelligence communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal procedures. Management should establish the responsibility and authority of security personnel and system administrators for monitoring. Additionally, management should review and approve the tools used and the conditions for use. Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies. Monitoring should address incoming and outgoing network traffic, seeking to identify malicious activity and data exfiltration. Additionally, the monitoring process should be established and documented to independently monitor administrators and other	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8		MON-01
III.B	N/A	Threat Monitoring Threat monitoring policies should provide for continual and ad hoc monitoring of threat intelligence communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal procedures. Management should establish the responsibility and authority of security personnel and system administrators for monitoring. Additionally, management should review and approve the tools used and the conditions for use. Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies. Monitoring should address incoming and outgoing network traffic, seeking to identify malicious activity and data exfiltration. Additionally, the monitoring process should be established and documented to independently monitor administrators and other	Functional	Intersects With	Privileged User Oversight	MON-14.2	Mechanisms exist to implement enhanced activity monitoring for privileged users.	5		MON-01.15

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
III.B	N/A	Threat Monitoring Threat monitoring policies should provide for continual and ad hoc monitoring of threat intelligence communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal procedures. Management should establish the responsibility and authority of security personnel and system administrators for monitoring. Additionally, management should review and approve the tools used and the conditions for use. Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies. Monitoring should address incoming and outgoing network traffic, seeking to identify malicious activity and data exfiltration. Additionally, the monitoring process should be established and documented to independently monitor administrators and other	Functional	Intersects With	Monitoring For Information Disclosure	MON-19	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	5		MON-11
III.B	N/A	Threat Monitoring Threat monitoring policies should provide for continual and ad hoc monitoring of threat intelligence communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal procedures. Management should establish the responsibility and authority of security personnel and system administrators for monitoring. Additionally, management should review and approve the tools used and the conditions for use. Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies. Monitoring should address incoming and outgoing network traffic, seeking to identify malicious activity and data exfiltration. Additionally, the monitoring process should be established and documented to independently monitor administrators and other	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5		MON-01.3
III.B	N/A	Threat Monitoring Threat monitoring policies should provide for continual and ad hoc monitoring of threat intelligence communications and systems, effective incident detection and response, and the use of monitoring reports in subsequent legal procedures. Management should establish the responsibility and authority of security personnel and system administrators for monitoring. Additionally, management should review and approve the tools used and the conditions for use. Threat monitoring should address indicators of vulnerabilities, attacks, compromised systems, and suspicious users, such as those who do not comply with or seek to evade security policies. Monitoring should address incoming and outgoing network traffic, seeking to identify malicious activity and data exfiltration. Additionally, the monitoring process should be established and documented to independently monitor administrators and other	Functional	Intersects With	Dynamic Threat Awareness	THR-03	Mechanisms exist to determine and maintain ongoing awareness of the current cyber threat environment.	3		THR-01.1
III.C	N/A	Incident Identification and Assessment Action Summary Management should have a process to enable the following: • Identify indicators of compromise. • Analyze the event associated with the indicators. • Classify the event. • Escalate the event consistent with the classification. • Report internally and externally as appropriate. Incident identification involves indicators and analysis. External indicators may arise through contact with customers, law enforcement, card organizations (e.g., credit or payment cards), other financial institutions, media, or others. Internal indicators may arise when internal users contact the help desk, IT operations follows up on anomalies, or security operations follows up on anomalies identified through security devices and network and systems activity. Indicators may also arise through the use of "hunt teams," or dedicated analysts who actively search for indicators of compromise. Examples of technology-based intrusion identification systems and tools include the following: • Threat intelligence data feeds (e.g., STIX/TAXII).60 • Intrusion detection and prevention systems for networks and hosts. • End-point visibility tools (tools that can identify the function of end points and which end points contain or have access to sensitive information). • DLP tools. • Log correlation and analysis tools. • File integrity tools. • Malware detection tools. • Network behavior analysis systems. • "Big data" tools and analytics that aggregate and allow pre-formed and ad hoc analysis. Technology-based indicators of compromise generally are anomalies in host state, host activity, and network traffic. A few examples are unexpected (1) processes, (2) changes to files, (3) packet source or destination, (4) protocols, (5) ports, (6) encryption, (7) log-ins, and (8) packet content. Other indicators include alerts triggered by black lists in anti-virus and network- monitoring products. Management should have a process for identifying indicators of compromise and rapidly reporting those	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5		IRO-02.4
III.C	N/A	Incident Identification and Assessment Action Summary Management should have a process to enable the following: • Identify indicators of compromise. • Analyze the event associated with the indicators. • Classify the event. • Escalate the event consistent with the classification. • Report internally and externally as appropriate. Incident identification involves indicators and analysis. External indicators may arise through contact with customers, law enforcement, card organizations (e.g., credit or payment cards), other financial institutions, media, or others. Internal indicators may arise when internal users contact the help desk, IT operations follows up on anomalies, or security operations follows up on anomalies identified through security devices and network and systems activity. Indicators may also arise through the use of "hunt teams," or dedicated analysts who actively search for indicators of compromise. Examples of technology-based intrusion identification systems and tools include the following: • Threat intelligence data feeds (e.g., STIX/TAXII).60 • Intrusion detection and prevention systems for networks and hosts. • End-point visibility tools (tools that can identify the function of end points and which end points contain or have access to sensitive information). • DLP tools. • Log correlation and analysis tools. • File integrity tools. • Malware detection tools. • Network behavior analysis systems. • "Big data" tools and analytics that aggregate and allow pre-formed and ad hoc analysis. Technology-based indicators of compromise generally are anomalies in host state, host activity, and network traffic. A few examples are unexpected (1) processes, (2) changes to files, (3) packet source or destination, (4) protocols, (5) ports, (6) encryption, (7) log-ins, and (8) packet content. Other indicators include alerts triggered by black lists in anti-virus and network- monitoring products. Management should have a process for identifying indicators of compromise and rapidly reporting those	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-05	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5		IRO-03

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
III.C	N/A	Incident Identification and Assessment Action Summary Management should have a process to enable the following: • Identify indicators of compromise. • Analyze the event associated with the indicators. • Classify the event. • Escalate the event consistent with the classification. • Report internally and externally as appropriate. Incident identification involves indicators and analysis. External indicators may arise through contact with customers, law enforcement, card organizations (e.g., credit or payment cards), other financial institutions, media, or others. Internal indicators may arise when internal users contact the help desk, IT operations follows up on anomalies, or security operations follows up on anomalies identified through security devices and network and systems activity. Indicators may also arise through the use of "hunt teams," or dedicated analysts who actively search for indicators of compromise. Examples of technology-based intrusion identification systems and tools include the following: • Threat intelligence data feeds (e.g., STIX/TAXII).60 • Intrusion detection and prevention systems for networks and hosts. • End-point visibility tools (tools that can identify the function of end points and which end points contain or have access to sensitive information). • DLP tools. • Log correlation and analysis tools. • File integrity tools. • Malware detection tools. • Network behavior analysis systems. • "Big data" tools and analytics that aggregate and allow pre-formed and ad hoc analysis. Technology-based indicators of compromise generally are anomalies in host state, host activity, and network traffic. A few examples are unexpected (1) processes, (2) changes to files, (3) packet source or destination, (4) protocols, (5) ports, (6) encryption, (7) log-ins, and (8) packet content. Other indicators include alerts triggered by black lists in anti-virus and network- monitoring products. Management should have a process for identifying indicators of compromise and rapidly reporting those	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8		IRO-02
III.C	N/A	Incident Identification and Assessment Action Summary Management should have a process to enable the following: • Identify indicators of compromise. • Analyze the event associated with the indicators. • Classify the event. • Escalate the event consistent with the classification. • Report internally and externally as appropriate. Incident identification involves indicators and analysis. External indicators may arise through contact with customers, law enforcement, card organizations (e.g., credit or payment cards), other financial institutions, media, or others. Internal indicators may arise when internal users contact the help desk, IT operations follows up on anomalies, or security operations follows up on anomalies identified through security devices and network and systems activity. Indicators may also arise through the use of "hunt teams," or dedicated analysts who actively search for indicators of compromise. Examples of technology-based intrusion identification systems and tools include the following: • Threat intelligence data feeds (e.g., STIX/TAXII).60 • Intrusion detection and prevention systems for networks and hosts. • End-point visibility tools (tools that can identify the function of end points and which end points contain or have access to sensitive information). • DLP tools. • Log correlation and analysis tools. • File integrity tools. • Malware detection tools. • Network behavior analysis systems. • "Big data" tools and analytics that aggregate and allow pre-formed and ad hoc analysis. Technology-based indicators of compromise generally are anomalies in host state, host activity, and network traffic. A few examples are unexpected (1) processes, (2) changes to files, (3) packet source or destination, (4) protocols, (5) ports, (6) encryption, (7) log-ins, and (8) packet content. Other indicators include alerts triggered by black lists in anti-virus and network- monitoring products. Management should have a process for identifying indicators of compromise and rapidly reporting those	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
III.C	N/A	Incident Identification and Assessment Action Summary Management should have a process to enable the following: • Identify indicators of compromise. • Analyze the event associated with the indicators. • Classify the event. • Escalate the event consistent with the classification. • Report internally and externally as appropriate. Incident identification involves indicators and analysis. External indicators may arise through contact with customers, law enforcement, card organizations (e.g., credit or payment cards), other financial institutions, media, or others. Internal indicators may arise when internal users contact the help desk, IT operations follows up on anomalies, or security operations follows up on anomalies identified through security devices and network and systems activity. Indicators may also arise through the use of "hunt teams," or dedicated analysts who actively search for indicators of compromise. Examples of technology-based intrusion identification systems and tools include the following: • Threat intelligence data feeds (e.g., STIX/TAXII).60 • Intrusion detection and prevention systems for networks and hosts. • End-point visibility tools (tools that can identify the function of end points and which end points contain or have access to sensitive information). • DLP tools. • Log correlation and analysis tools. • File integrity tools. • Malware detection tools. • Network behavior analysis systems. • "Big data" tools and analytics that aggregate and allow pre-formed and ad hoc analysis. Technology-based indicators of compromise generally are anomalies in host state, host activity, and network traffic. A few examples are unexpected (1) processes, (2) changes to files, (3) packet source or destination, (4) protocols, (5) ports, (6) encryption, (7) log-ins, and (8) packet content. Other indicators include alerts triggered by black lists in anti-virus and network- monitoring products. Management should have a process for identifying indicators of compromise and rapidly reporting those	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-17	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	3		MON-11.3

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
III.D	N/A	Incident Response Management should have an incident response program.61 The goal of incident response is to minimize damage to the institution and its customers. The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate, containing the incident, coordinating with law 61 See also "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," supplementing the Information Security Standards. enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience of the institution. The response involves a combination of people and technologies. The quality of incident response is attributable to the institution's culture, policies, procedures, and training. Incident response is also a function of the relationships the institution formed before the incident with law enforcement, incident response consultants and attorneys, information-sharing entities (e.g., FS- ISAC), and others. Management should prepare for potential incidents by developing an incident response plan that is comprehensive, coordinated, and integrated with existing institution policies, procedures, and training. To validate the effectiveness of the institution's incident response program, management should periodically test it through different test types, including scenario planning and tabletop testing, and perform the tests with appropriate internal and external parties. Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort. Additionally, management should define thresholds	Functional	Intersects With	Incident Response Operations	IRO-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	8		IRO-01
III.D	N/A	Incident Response Management should have an incident response program.61 The goal of incident response is to minimize damage to the institution and its customers. The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate, containing the incident, coordinating with law 61 See also "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," supplementing the Information Security Standards. enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience of the institution. The response involves a combination of people and technologies. The quality of incident response is attributable to the institution's culture, policies, procedures, and training. Incident response is also a function of the relationships the institution formed before the incident with law enforcement, incident response consultants and attorneys, information-sharing entities (e.g., FS- ISAC), and others. Management should prepare for potential incidents by developing an incident response plan that is comprehensive, coordinated, and integrated with existing institution policies, procedures, and training. To validate the effectiveness of the institution's incident response program, management should periodically test it through different test types, including scenario planning and tabletop testing, and perform the tests with appropriate internal and external parties. Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort. Additionally, management should define thresholds	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.	5		IRO-04
III.D	N/A	Incident Response Management should have an incident response program.61 The goal of incident response is to minimize damage to the institution and its customers. The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate, containing the incident, coordinating with law 61 See also "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," supplementing the Information Security Standards. enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience of the institution. The response involves a combination of people and technologies. The quality of incident response is attributable to the institution's culture, policies, procedures, and training. Incident response is also a function of the relationships the institution formed before the incident with law enforcement, incident response consultants and attorneys, information-sharing entities (e.g., FS- ISAC), and others. Management should prepare for potential incidents by developing an incident response plan that is comprehensive, coordinated, and integrated with existing institution policies, procedures, and training. To validate the effectiveness of the institution's incident response program, management should periodically test it through different test types, including scenario planning and tabletop testing, and perform the tests with appropriate internal and external parties. Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort. Additionally, management should define thresholds	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

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 - FFIEC IT Examination Handbook - Information Security (September 2016)**
Focal Document URL:	https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL:	https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
III.D	N/A	Incident Response Management should have an incident response program.61 The goal of incident response is to minimize damage to the institution and its customers. The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate, containing the incident, coordinating with law 61 See also "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," supplementing the Information Security Standards. enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience of the institution. The response involves a combination of people and technologies. The quality of incident response is attributable to the institution's culture, policies, procedures, and training. Incident response is also a function of the relationships the institution formed before the incident with law enforcement, incident response consultants and attorneys, information-sharing entities (e.g., FS- ISAC), and others. Management should prepare for potential incidents by developing an incident response plan that is comprehensive, coordinated, and integrated with existing institution policies, procedures, and training. To validate the effectiveness of the institution's incident response program, management should periodically test it through different test types, including scenario planning and tabletop testing, and perform the tests with appropriate internal and external parties. Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort. Additionally, management should define thresholds	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5		IRO-07
III.D	N/A	Incident Response Management should have an incident response program.61 The goal of incident response is to minimize damage to the institution and its customers. The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate, containing the incident, coordinating with law 61 See also "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," supplementing the Information Security Standards. enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience of the institution. The response involves a combination of people and technologies. The quality of incident response is attributable to the institution's culture, policies, procedures, and training. Incident response is also a function of the relationships the institution formed before the incident with law enforcement, incident response consultants and attorneys, information-sharing entities (e.g., FS- ISAC), and others. Management should prepare for potential incidents by developing an incident response plan that is comprehensive, coordinated, and integrated with existing institution policies, procedures, and training. To validate the effectiveness of the institution's incident response program, management should periodically test it through different test types, including scenario planning and tabletop testing, and perform the tests with appropriate internal and external parties. Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort. Additionally, management should define thresholds	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
III.D	N/A	Incident Response Management should have an incident response program.61 The goal of incident response is to minimize damage to the institution and its customers. The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate, containing the incident, coordinating with law 61 See also "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," supplementing the Information Security Standards. enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience of the institution. The response involves a combination of people and technologies. The quality of incident response is attributable to the institution's culture, policies, procedures, and training. Incident response is also a function of the relationships the institution formed before the incident with law enforcement, incident response consultants and attorneys, information-sharing entities (e.g., FS- ISAC), and others. Management should prepare for potential incidents by developing an incident response plan that is comprehensive, coordinated, and integrated with existing institution policies, procedures, and training. To validate the effectiveness of the institution's incident response program, management should periodically test it through different test types, including scenario planning and tabletop testing, and perform the tests with appropriate internal and external parties. Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort. Additionally, management should define thresholds	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
IV	Examination Procedures	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
IV.A	Objectives and Procedures	N/A	Functional	No Relationship	N/A	N/A	N/A	0		

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
IV.A.1	N/A	Key Testing Factors Management should consider the following key factors when developing and implementing independent tests: • Scope. The tests and methods utilized, in the aggregate, should be sufficient to validate the effectiveness of the security process in identifying and appropriately controlling the risk from information security-related events. • Personnel. Technical testing is only as good as the personnel performing and supervising the test. Management should review qualifications of testing personnel to verify testers' capabilities are adequate to support the test objectives. • Notifications. Management should consider whom to inform within the institution about the timing and nature of the tests. The need for protection of institution systems and the potential for disruptive false alarms should be balanced against the need to test personnel reactions to unexpected activities. 62 See also Information Security Standards, section III.C.3, requiring each financial institution to test the key controls, systems, and procedures of its information security program using independent third parties or staff independent of those that develop or maintain the program. • Confidentiality, integrity, and availability. Management should carefully control information security tests to limit the risks to confidentiality, integrity, and system availability. Because testing may uncover sensitive customer information, management should use appropriate safeguards to protect such information. Management should ensure that employee and contract personnel who perform the tests or have access to the test results have passed appropriate background checks and that contract personnel are appropriately bonded. Because certain tests may pose more risk to system availability than other tests, management should have personnel who perform those tests maintain logs of testing actions. Those logs are helpful if the systems react unexpectedly. • Confidentiality of test plans and data. Because	Functional	Intersects With	Assessment Team Subject Matter Expertise	CPL-09	Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable: (1) Professional qualifications to perform the audit and/or assessment; and (2) Subject matter expertise to perform review, interview and test activities for in-scope People, Processes, Technologies, Data and/or Facilities (PPTDF).	5		CPL-01.6
IV.A.1	N/A	Key Testing Factors Management should consider the following key factors when developing and implementing independent tests: • Scope. The tests and methods utilized, in the aggregate, should be sufficient to validate the effectiveness of the security process in identifying and appropriately controlling the risk from information security-related events. • Personnel. Technical testing is only as good as the personnel performing and supervising the test. Management should review qualifications of testing personnel to verify testers' capabilities are adequate to support the test objectives. • Notifications. Management should consider whom to inform within the institution about the timing and nature of the tests. The need for protection of institution systems and the potential for disruptive false alarms should be balanced against the need to test personnel reactions to unexpected activities. 62 See also Information Security Standards, section III.C.3, requiring each financial institution to test the key controls, systems, and procedures of its information security program using independent third parties or staff independent of those that develop or maintain the program. • Confidentiality, integrity, and availability. Management should carefully control information security tests to limit the risks to confidentiality, integrity, and system availability. Because testing may uncover sensitive customer information, management should use appropriate safeguards to protect such information. Management should ensure that employee and contract personnel who perform the tests or have access to the test results have passed appropriate background checks and that contract personnel are appropriately bonded. Because certain tests may pose more risk to system availability than other tests, management should have personnel who perform those tests maintain logs of testing actions. Those logs are helpful if the systems react unexpectedly. • Confidentiality of test plans and data. Because	Functional	Intersects With	Assessment Rigor	CPL-12	Mechanisms exist to define the level of assessment rigor necessary to conduct a cybersecurity and/or data protection assessment.	3		CPL-03.5
IV.A.1	N/A	Key Testing Factors Management should consider the following key factors when developing and implementing independent tests: • Scope. The tests and methods utilized, in the aggregate, should be sufficient to validate the effectiveness of the security process in identifying and appropriately controlling the risk from information security-related events. • Personnel. Technical testing is only as good as the personnel performing and supervising the test. Management should review qualifications of testing personnel to verify testers' capabilities are adequate to support the test objectives. • Notifications. Management should consider whom to inform within the institution about the timing and nature of the tests. The need for protection of institution systems and the potential for disruptive false alarms should be balanced against the need to test personnel reactions to unexpected activities. 62 See also Information Security Standards, section III.C.3, requiring each financial institution to test the key controls, systems, and procedures of its information security program using independent third parties or staff independent of those that develop or maintain the program. • Confidentiality, integrity, and availability. Management should carefully control information security tests to limit the risks to confidentiality, integrity, and system availability. Because testing may uncover sensitive customer information, management should use appropriate safeguards to protect such information. Management should ensure that employee and contract personnel who perform the tests or have access to the test results have passed appropriate background checks and that contract personnel are appropriately bonded. Because certain tests may pose more risk to system availability than other tests, management should have personnel who perform those tests maintain logs of testing actions. Those logs are helpful if the systems react unexpectedly. • Confidentiality of test plans and data. Because	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

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
IV.A.1	N/A	Key Testing Factors Management should consider the following key factors when developing and implementing independent tests: • Scope. The tests and methods utilized, in the aggregate, should be sufficient to validate the effectiveness of the security process in identifying and appropriately controlling the risk from information security-related events. • Personnel. Technical testing is only as good as the personnel performing and supervising the test. Management should review qualifications of testing personnel to verify testers' capabilities are adequate to support the test objectives. • Notifications. Management should consider whom to inform within the institution about the timing and nature of the tests. The need for protection of institution systems and the potential for disruptive false alarms should be balanced against the need to test personnel reactions to unexpected activities. 62 See also Information Security Standards, section III.C.3, requiring each financial institution to test the key controls, systems, and procedures of its information security program using independent third parties or staff independent of those that develop or maintain the program. • Confidentiality, integrity, and availability. Management should carefully control information security tests to limit the risks to confidentiality, integrity, and system availability. Because testing may uncover sensitive customer information, management should use appropriate safeguards to protect such information. Management should ensure that employee and contract personnel who perform the tests or have access to the test results have passed appropriate background checks and that contract personnel are appropriately bonded. Because certain tests may pose more risk to system availability than other tests, management should have personnel who perform those tests maintain logs of testing actions. Those logs are helpful if the systems react unexpectedly. • Confidentiality of test plans and data. Because	Functional	Intersects With	Plan / Coordinate with Other Organizational Entities	IAO-04.1	Mechanisms exist to plan and coordinate Control Validation Testing (CVT) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	5		IAO-03.1
IV.A.2	Work Program	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
IV.A.2.a	N/A	Self-Assessments Periodic self-assessments typically should be performed by the organizational unit being assessed. Self-assessments capture subjective opinions on the achievement of objectives. Although they may provide valuable information related to perceived changes in the level of risk and effectiveness of controls, they are affected by the breadth and depth of the assessor's knowledge, the completeness and reliability of information used to complete the assessment, and the assessor's biases. Self-assessment frequency should be a function of the level of assurance needed by the institution, determined by the risk management process. Results from self- assessments can be informative to the overall test and evaluation process. Management should use the results to help strengthen the organizational unit's information security.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5		CPL-03.2
IV.A.2.a	N/A	Self-Assessments Periodic self-assessments typically should be performed by the organizational unit being assessed. Self-assessments capture subjective opinions on the achievement of objectives. Although they may provide valuable information related to perceived changes in the level of risk and effectiveness of controls, they are affected by the breadth and depth of the assessor's knowledge, the completeness and reliability of information used to complete the assessment, and the assessor's biases. Self-assessment frequency should be a function of the level of assurance needed by the institution, determined by the risk management process. Results from self- assessments can be informative to the overall test and evaluation process. Management should use the results to help strengthen the organizational unit's information security.	Functional	Intersects With	Assess Controls	GOV-11.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control are: (1) Designed to meet control objectives; (2) Implemented correctly; and (3) Operating as intended.	5		GOV-15.3
IV.A.2.a	N/A	Self-Assessments Periodic self-assessments typically should be performed by the organizational unit being assessed. Self-assessments capture subjective opinions on the achievement of objectives. Although they may provide valuable information related to perceived changes in the level of risk and effectiveness of controls, they are affected by the breadth and depth of the assessor's knowledge, the completeness and reliability of information used to complete the assessment, and the assessor's biases. Self-assessment frequency should be a function of the level of assurance needed by the institution, determined by the risk management process. Results from self- assessments can be informative to the overall test and evaluation process. Management should use the results to help strengthen the organizational unit's information security.	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.	3		IAO-02
IV.A.2.b	N/A	Penetration Tests A penetration test subjects a system to real-world attacks selected and conducted by the testers. A penetration test targets systems and users to identify weaknesses in business processes and technical controls. The test mimics a threat source's search for and exploitation of vulnerabilities to demonstrate a potential for loss. Some tests focus on only a subset of the institution's systems and may not accurately simulate a determined threat actor. There are many types of penetration tests (e.g., network, client-side, web application, and social engineering), and management should determine the level and types of tests employed to ensure effective and comprehensive coverage. The frequency and scope of a penetration test should be a function of the level of assurance needed by the institution and determined by the risk assessment process. The test can be performed internally by independent groups, internally by the organizational unit, or by an independent third party. Management should determine the level of independence required of the test.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8		VPM-07
IV.A.2.b	N/A	Penetration Tests A penetration test subjects a system to real-world attacks selected and conducted by the testers. A penetration test targets systems and users to identify weaknesses in business processes and technical controls. The test mimics a threat source's search for and exploitation of vulnerabilities to demonstrate a potential for loss. Some tests focus on only a subset of the institution's systems and may not accurately simulate a determined threat actor. There are many types of penetration tests (e.g., network, client-side, web application, and social engineering), and management should determine the level and types of tests employed to ensure effective and comprehensive coverage. The frequency and scope of a penetration test should be a function of the level of assurance needed by the institution and determined by the risk assessment process. The test can be performed internally by independent groups, internally by the organizational unit, or by an independent third party. Management should determine the level of independence required of the test.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-19	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5		VPM-07.1

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
IV.A.2.c	N/A	Vulnerability Assessments A vulnerability assessment is a process that defines, identifies, and classifies the vulnerabilities in a computer, network, or communications infrastructure. Technical vulnerabilities can be identified through the use of scanners and other tools. Scanners search for known vulnerabilities (e.g., Mitre's CVE) or for known vulnerability classes (e.g., Structured Query Language [SQL] injection and cross-site scripting). They also can search for compliance with approved configurations. Scanners identify vulnerabilities by inspecting network traffic or hosts. When inspecting hosts, they may require agents to be placed on the hosts with high-level access. If host agents are required, the security over the use of credentials in the scan should be a prime consideration for management. Similar to penetration testing, the frequency of the performance of vulnerability assessments should be determined by the risk management process. Scanners and other tools can be run continuously, generating metrics that are reported and acted upon continuously. Alternatively, they can be run periodically. Vulnerability assessments can be performed internally or by external testers, but they are often run as part of internal testing processes.	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
IV.A.2.c	N/A	Vulnerability Assessments A vulnerability assessment is a process that defines, identifies, and classifies the vulnerabilities in a computer, network, or communications infrastructure. Technical vulnerabilities can be identified through the use of scanners and other tools. Scanners search for known vulnerabilities (e.g., Mitre's CVE) or for known vulnerability classes (e.g., Structured Query Language [SQL] injection and cross-site scripting). They also can search for compliance with approved configurations. Scanners identify vulnerabilities by inspecting network traffic or hosts. When inspecting hosts, they may require agents to be placed on the hosts with high-level access. If host agents are required, the security over the use of credentials in the scan should be a prime consideration for management. Similar to penetration testing, the frequency of the performance of vulnerability assessments should be determined by the risk management process. Scanners and other tools can be run continuously, generating metrics that are reported and acted upon continuously. Alternatively, they can be run periodically. Vulnerability assessments can be performed internally or by external testers, but they are often run as part of internal testing processes.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8		VPM-06
IV.A.2.c	N/A	Vulnerability Assessments A vulnerability assessment is a process that defines, identifies, and classifies the vulnerabilities in a computer, network, or communications infrastructure. Technical vulnerabilities can be identified through the use of scanners and other tools. Scanners search for known vulnerabilities (e.g., Mitre's CVE) or for known vulnerability classes (e.g., Structured Query Language [SQL] injection and cross-site scripting). They also can search for compliance with approved configurations. Scanners identify vulnerabilities by inspecting network traffic or hosts. When inspecting hosts, they may require agents to be placed on the hosts with high-level access. If host agents are required, the security over the use of credentials in the scan should be a prime consideration for management. Similar to penetration testing, the frequency of the performance of vulnerability assessments should be determined by the risk management process. Scanners and other tools can be run continuously, generating metrics that are reported and acted upon continuously. Alternatively, they can be run periodically. Vulnerability assessments can be performed internally or by external testers, but they are often run as part of internal testing processes.	Functional	Intersects With	Breadth / Depth of Coverage For Vulnerability Scanning	VPM-12.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	3		VPM-06.2
IV.A.2.d	N/A	Audits Independent internal departments or third parties typically perform audits. Audits should review every aspect of the information security program, the environment in which the program runs, and outputs of the program. Audits should assess the reasonableness and appropriateness of, and compliance with, policies, standards, and procedures; report on information security activity and control deficiencies to decision makers; identify root causes and recommendations to address deficiencies; and test the effectiveness of controls within the program. Internal audit should track the results and the remediation of control deficiencies reported in audits and additional technical reviews, such as penetration tests and vulnerability assessments. Refer to the IT Handbook's "Audit" booklet for more information.	Functional	Intersects With	Non-Conformity Corrective Action	CPL-06.1	Mechanisms exist to implement corrective action to remediate instances of non-conformity with applicable statutory, regulatory, and/or contractual compliance obligations.	5		CPL-02.3
IV.A.2.d	N/A	Audits Independent internal departments or third parties typically perform audits. Audits should review every aspect of the information security program, the environment in which the program runs, and outputs of the program. Audits should assess the reasonableness and appropriateness of, and compliance with, policies, standards, and procedures; report on information security activity and control deficiencies to decision makers; identify root causes and recommendations to address deficiencies; and test the effectiveness of controls within the program. Internal audit should track the results and the remediation of control deficiencies reported in audits and additional technical reviews, such as penetration tests and vulnerability assessments. Refer to the IT Handbook's "Audit" booklet for more information.	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	8		CPL-02.1
IV.A.2.d	N/A	Audits Independent internal departments or third parties typically perform audits. Audits should review every aspect of the information security program, the environment in which the program runs, and outputs of the program. Audits should assess the reasonableness and appropriateness of, and compliance with, policies, standards, and procedures; report on information security activity and control deficiencies to decision makers; identify root causes and recommendations to address deficiencies; and test the effectiveness of controls within the program. Internal audit should track the results and the remediation of control deficiencies reported in audits and additional technical reviews, such as penetration tests and vulnerability assessments. Refer to the IT Handbook's "Audit" booklet for more information.	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5		CPL-02.2
IV.A.2.d	N/A	Audits Independent internal departments or third parties typically perform audits. Audits should review every aspect of the information security program, the environment in which the program runs, and outputs of the program. Audits should assess the reasonableness and appropriateness of, and compliance with, policies, standards, and procedures; report on information security activity and control deficiencies to decision makers; identify root causes and recommendations to address deficiencies; and test the effectiveness of controls within the program. Internal audit should track the results and the remediation of control deficiencies reported in audits and additional technical reviews, such as penetration tests and vulnerability assessments. Refer to the IT Handbook's "Audit" booklet for more information.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05

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 - FFIEC IT Examination Handbook - Information Security (September 2016)
Focal Document URL: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-ffiec-iteh-2016.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 #
IV.A.3	N/A	Independence of Tests and Audits Institutions frequently use independent organizations to test aspects of their information security programs. Independent tests have the potential to reduce bias, increase capabilities, and increase knowledge about threats and technologies. Independence gives credibility to the test results. To be considered independent, testing personnel should not be responsible for the design, installation, maintenance, and operation of the tested system, or the policies and procedures that guide its operation. The reports generated from the tests should be prepared by individuals who similarly are independent.	Functional	Intersects With	Independent Assessors	CPL-08	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5		CPL-03.1
IV.A.3	N/A	Independence of Tests and Audits Institutions frequently use independent organizations to test aspects of their information security programs. Independent tests have the potential to reduce bias, increase capabilities, and increase knowledge about threats and technologies. Independence gives credibility to the test results. To be considered independent, testing personnel should not be responsible for the design, installation, maintenance, and operation of the tested system, or the policies and procedures that guide its operation. The reports generated from the tests should be prepared by individuals who similarly are independent.	Functional	Subset Of	Assessor Independence	IAO-06	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments.	10		IAO-02.1
IV.A.4	N/A	Assurance Reporting Reporting of self-assessments, penetration tests, vulnerability assessments, and audits supports management decision making. Those decisions may support a range of ITRM activities, including the prioritization and funding of resource allocations and improvement to existing information security policies and procedures. Management should provide reports that are timely, complete, transparent, and relevant to management decisions. The reports should prioritize risk and findings in the order of importance, suggest options for remediation, and highlight repeat issues. Additionally, reports should address root causes. The reporting should be to individuals with authority and responsibility to act on the reports and to those accountable for the outcomes, as well as those responsible for advising or influencing risk decisions. Reporting should trigger appropriate, timely, and reliable escalation and response procedures. Summary reports should be made available to the board as	Functional	Intersects With	Executive Leadership Oversight of Security, Compliance & Resilience Controls	CPL-07	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	3		CPL-02
IV.A.4	N/A	Assurance Reporting Reporting of self-assessments, penetration tests, vulnerability assessments, and audits supports management decision making. Those decisions may support a range of ITRM activities, including the prioritization and funding of resource allocations and improvement to existing information security policies and procedures. Management should provide reports that are timely, complete, transparent, and relevant to management decisions. The reports should prioritize risk and findings in the order of importance, suggest options for remediation, and highlight repeat issues. Additionally, reports should address root causes. The reporting should be to individuals with authority and responsibility to act on the reports and to those accountable for the outcomes, as well as those responsible for advising or influencing risk decisions. Reporting should trigger appropriate, timely, and reliable escalation and response procedures. Summary reports should be made available to the board as	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2
IV.A.4	N/A	Assurance Reporting Reporting of self-assessments, penetration tests, vulnerability assessments, and audits supports management decision making. Those decisions may support a range of ITRM activities, including the prioritization and funding of resource allocations and improvement to existing information security policies and procedures. Management should provide reports that are timely, complete, transparent, and relevant to management decisions. The reports should prioritize risk and findings in the order of importance, suggest options for remediation, and highlight repeat issues. Additionally, reports should address root causes. The reporting should be to individuals with authority and responsibility to act on the reports and to those accountable for the outcomes, as well as those responsible for advising or influencing risk decisions. Reporting should trigger appropriate, timely, and reliable escalation and response procedures. Summary reports should be made available to the board as appropriate.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	5		IAO-05
IV.A.4	N/A	Assurance Reporting Reporting of self-assessments, penetration tests, vulnerability assessments, and audits supports management decision making. Those decisions may support a range of ITRM activities, including the prioritization and funding of resource allocations and improvement to existing information security policies and procedures. Management should provide reports that are timely, complete, transparent, and relevant to management decisions. The reports should prioritize risk and findings in the order of importance, suggest options for remediation, and highlight repeat issues. Additionally, reports should address root causes. The reporting should be to individuals with authority and responsibility to act on the reports and to those accountable for the outcomes, as well as those responsible for advising or influencing risk decisions. Reporting should trigger appropriate, timely, and reliable escalation and response procedures. Summary reports should be made available to the board as	Functional	Intersects With	Security Assessment Report (SAR)	IAO-13	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5		IAO-02.4