NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.3
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: Farm Credit Administration (FCA) Cyber Risk Management
Focal Document URL: https://www.federalregister.gov/documents/2023/12/11/2023-27102/cyber-risk-management#sectno-citation-609.905
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-us-fed-fca-crm.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 (optional)	Notes (optional)
609.905	In general.	Farm Credit System (System) institutions must engage in appropriate risk management practices to ensure safety and soundness of their operations. A System institution's board and management must maintain and document effective policies, procedures, and controls to mitigate cyber risks. This includes establishing an appropriate vulnerability management program to monitor cyber threats, mitigate any known vulnerabilities, and establish appropriate reporting mechanisms to the institution's board and the Farm Credit Administration (FCA). The vulnerability management programs should be commensurate with the size, risk profile, and complexity of the institution and based on sound industry standards and practices.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
609.930	Cyber risk management.	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Subset Of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	8	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	8	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control are implemented correctly and are operating as intended.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications and/or Services (TAAS) under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity and data protection controls are operating as intended.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	8	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Management Resourcing	RSK-01.2	Mechanisms exist to reduce the magnitude or likelihood of potential impacts by resourcing the capability required to manage technology-related risks.	3	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Assessment	RSK-04	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).	8	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed.	5	
609.930(a)	Cyber risk management program.	Each System institution must implement a comprehensive, written cyber risk management program consistent with the size, risk profile, and complexity of the institution's operations. The program must ensure controls exist to protect the security and confidentiality of current, former, and potential customer and employee information, protect against reasonably anticipated cyber threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
609.930(b)	Role of the board.	Each year, the board of directors of each System institution or an appropriate committee of the board must:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
609.930(b)(1)	N/A	Approve a written cyber risk program. The program must be consistent with industry standards to ensure the institution's safety and soundness and compliance with law and regulations;	Functional	Subset Of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
609.930(b)(2)	N/A	Oversee the development, implementation, and maintenance of the institution's cyber risk program; and	Functional	Subset Of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
609.930(b)(3)	N/A	Determine necessary expertise for executing the cyber risk management plan and, where practical, delegate day-to-day responsibilities to management and employees.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	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 cybersecurity and data protection program.	8	
609.930(b)(3)	N/A	Determine necessary expertise for executing the cyber risk management plan and, where practical, delegate day-to-day responsibilities to management and employees.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
609.930(b)(3)	N/A	Determine necessary expertise for executing the cyber risk management plan and, where practical, delegate day-to-day responsibilities to management and employees.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	8	
609.930(b)(3)	N/A	Determine necessary expertise for executing the cyber risk management plan and, where practical, delegate day-to-day responsibilities to management and employees.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
609.930(b)(3)	N/A	Determine necessary expertise for executing the cyber risk management plan and, where practical, delegate day-to-day responsibilities to management and employees.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	8	
609.930(c)	Cyber risk program.	Each institution's cyber risk program must, at a minimum:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
609.930(c)(1)	N/A	Include an annual risk assessment of the internal and external factors likely to affect the institution. The risk assessment, at a minimum, must:	Functional	Equal	Risk Assessment	RSK-04	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).	10	
609.930(c)(1)(i)	N/A	Identify and assess internal and external factors that could result in unauthorized disclosure, misuse, alteration, or destruction of current, former, and potential customer and employee information or information systems; and	Functional	Subset Of	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	10	
609.930(c)(1)(ii)	N/A	Assess the sufficiency of policies, procedures, internal controls, and other practices in place to mitigate risks.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
609.930(c)(1)(ii)	N/A	Assess the sufficiency of policies, procedures, internal controls, and other practices in place to mitigate risks.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
609.930(c)(1)(ii)	N/A	Assess the sufficiency of policies, procedures, internal controls, and other practices in place to mitigate risks.	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	3	
609.930(c)(1)(ii)	N/A	Assess the sufficiency of policies, procedures, internal controls, and other practices in place to mitigate risks.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards.	5	
609.930(c)(2)	N/A	Identify systems and software vulnerabilities, prioritize the vulnerabilities and the affected systems based on risk, and perform timely remediation. The particular security measures an institution adopts will depend upon the size, risk profile, and complexity of the institution's operations and activities.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
609.930(c)(2)	N/A	Identify systems and software vulnerabilities, prioritize the vulnerabilities and the affected systems based on risk, and perform timely remediation. The particular security measures an institution adopts will depend upon the size, risk profile, and complexity of the institution's operations and activities.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	8	
609.930(c)(2)	N/A	Identify systems and software vulnerabilities, prioritize the vulnerabilities and the affected systems based on risk, and perform timely remediation. The particular security measures an institution adopts will depend upon the size, risk profile, and complexity of the institution's operations and activities.	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	8	
609.930(c)(2)	N/A	Identify systems and software vulnerabilities, prioritize the vulnerabilities and the affected systems based on risk, and perform timely remediation. The particular security measures an institution adopts will depend upon the size, risk profile, and complexity of the institution's operations and activities.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
609.930(c)(2)	N/A	Identify systems and software vulnerabilities, prioritize the vulnerabilities and the affected systems based on risk, and perform timely remediation. The particular security measures an institution adopts will depend upon the size, risk profile, and complexity of the institution's operations and activities.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8	
609.930(c)(3)	N/A	Maintain an incident response plan that contains procedures the institution must implement when it suspects or detects unauthorized access to current, former, or potential customer, employee, or other sensitive or confidential information. An institution's incident response plan must be reviewed and updated periodically, but at least annually, to address new threats, concerns, and evolving technology. The incident response plan must contain procedures for:	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
609.930(c)(3)	N/A	Maintain an incident response plan that contains procedures the institution must implement when it suspects or detects unauthorized access to current, former, or potential customer, employee, or other sensitive or confidential information. An institution's incident response plan must be reviewed and updated periodically, but at least annually, to address new threats, concerns, and evolving technology. The incident response plan must contain procedures for:	Functional	Intersects With	Incident Handling	IRO-02	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	
609.930(c)(3)	N/A	Maintain an incident response plan that contains procedures the institution must implement when it suspects or detects unauthorized access to current, former, or potential customer, employee, or other sensitive or confidential information. An institution's incident response plan must be reviewed and updated periodically, but at least annually, to address new threats, concerns, and evolving technology. The incident response plan must contain procedures for:	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8	
609.930(c)(3)	N/A	Maintain an incident response plan that contains procedures the institution must implement when it suspects or detects unauthorized access to current, former, or potential customer, employee, or other sensitive or confidential information. An institution's incident response plan must be reviewed and updated periodically, but at least annually, to address new threats, concerns, and evolving technology. The incident response plan must contain procedures for:	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	8	
609.930(c)(3)(i)	N/A	Assessing the nature and scope of an incident, and identifying what information systems and types of information have been accessed or misused;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
609.930(c)(3)(ii)	N/A	Acting to contain the incident while preserving records and other evidence;	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
609.930(c)(3)(iii)	N/A	Resuming business activities during intrusion response;	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	8	
609.930(c)(3)(iii)	N/A	Resuming business activities during intrusion response;	Functional	Intersects With	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
609.930(c)(3)(iii)	N/A	Resuming business activities during intrusion response;	Functional	Intersects With	Incident Handling	IRO-02	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	
609.930(c)(3)(iv)	N/A	Notifying the institution's board of directors when the institution learns of an incident involving unauthorized access to or use of sensitive or confidential customer, and/or employee information, or unauthorized access to financial institution information including proprietary information;	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	8	
609.930(c)(3)(v)	N/A	Notifying FCA as soon as possible or no later than 36 hours after the institution determines that an incident has occurred; and	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	
609.930(c)(3)(v)	N/A	Notifying FCA as soon as possible or no later than 36 hours after the institution determines that an incident has occurred; and	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	8	
609.930(c)(3)(vi)	N/A	Notifying former, current, or potential customers and employees and known visitors to your website of an incident when warranted, and in accordance with state and federal laws.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work.	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity and data protection policies and provide acknowledgement.	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Subset Of	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
609.930(c)(4)	N/A	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
609.930(c)(5)	N/A	Include policies for vendor management and oversight. Each institution, at a minimum, must:	Functional	Subset Of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
609.930(c)(5)	N/A	Include policies for vendor management and oversight. Each institution, at a minimum, must:	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	8	
609.930(c)(5)(i)	N/A	Exercise appropriate due diligence in selecting vendors;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3	
609.930(c)(5)(i)	N/A	Exercise appropriate due diligence in selecting vendors;	Functional	Intersects With	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	3	
609.930(c)(5)(i)	N/A	Exercise appropriate due diligence in selecting vendors;	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
609.930(c)(5)(i)	N/A	Exercise appropriate due diligence in selecting vendors;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8	
609.930(c)(5)(ii)	N/A	Negotiate contract provisions, when feasible, that facilitate effective risk management and oversight and specify the expectations and obligations of both parties;	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
609.930(c)(5)(ii)	N/A	Negotiate contract provisions, when feasible, that facilitate effective risk management and oversight and specify the expectations and obligations of both parties;	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	8	
609.930(c)(5)(iii)	N/A	Conduct a vendor risk assessment on all vendors; and	Functional	Equal	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	10	
609.930(c)(5)(iv)	N/A	Monitor its IT and cyber risk management related vendors to ensure they have satisfied agreed upon expectations and deliverables. Monitoring may include reviewing audits, summaries of test results, or other equivalent evaluations of its vendors.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	8	
609.930(c)(6)	N/A	Maintain robust internal controls by regularly testing the key controls, systems, and procedures of the cyber risk management program.	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	8	
609.930(c)(6)	N/A	Maintain robust internal controls by regularly testing the key controls, systems, and procedures of the cyber risk management program.	Functional	Subset Of	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	10	
609.930(c)(6)	N/A	Maintain robust internal controls by regularly testing the key controls, systems, and procedures of the cyber risk management program.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	8	
609.930(c)(6)	N/A	Maintain robust internal controls by regularly testing the key controls, systems, and procedures of the cyber risk management program.	Functional	Intersects With	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of cybersecurity and data protection controls to evaluate conformity with the organization's documented policies, standards and procedures.	8	
609.930(c)(6)(i)	N/A	The frequency and nature of such tests are to be determined by the institution's risk assessment.	Functional	Subset Of	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	10	
609.930(c)(6)(ii)	N/A	Tests must be conducted or reviewed by independent third parties or staff independent of those who develop or maintain the cyber risk management program.	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity and data protection controls at planned intervals or when the system, service or project undergoes significant changes.	8	
609.930(c)(6)(iii)	N/A	Internal systems and controls must provide reasonable assurances that System institutions will prevent, detect, and remediate material deficiencies on a timely basis.	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
609.930(c)(6)(iii)	N/A	Internal systems and controls must provide reasonable assurances that System institutions will prevent, detect, and remediate material deficiencies on a timely basis.	Functional	Intersects With	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards.	5	
609.930(d)	Privacy.	Institutions must consider privacy and other legal compliance issues, including but not limited to, the privacy and security of System institution information; current, former, and potential borrower information; and employee information, as well as compliance with statutory requirements for the use of electronic media.	Functional	Subset Of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
609.930(d)	Privacy.	Institutions must consider privacy and other legal compliance issues, including but not limited to, the privacy and security of System institution information; current, former, and potential borrower information; and employee information, as well as compliance with statutory requirements for the use of electronic media.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
609.930(d)	Privacy.	Institutions must consider privacy and other legal compliance issues, including but not limited to, the privacy and security of System institution information; current, former, and potential borrower information; and employee information, as well as compliance with statutory requirements for the use of electronic media.	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
609.930(e)	Board reporting requirements.	At a minimum, each institution must report quarterly to its board or an appropriate committee of the board. The report must contain material matters related to the institution's cyber risk management program, including specific risks and threats.	Functional	Subset Of	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and data protection program.	10	
609.935	Business planning.	The annually approved business plan required under subpart J of part 618 of this chapter, and § 652.60 of this chapter for System institutions and the Federal Agricultural Mortgage Corporation, respectively, must include a technology plan that, at a minimum:	Functional	Subset Of	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and data protection-specific business plan and set of objectives to achieve that plan.	10	
609.935(a)	N/A	Describes the institution's intended technology goals, performance measures, and objectives;	Functional	Subset Of	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and data protection-specific business plan and set of objectives to achieve that plan.	10	
609.935(b)	N/A	Details the technology budget;	Functional	Subset Of	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	10	
609.935(c)	N/A	Identifies and assesses the adequacy of the institution's entire cyber risk management program, including proposed technology changes;	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
609.935(d)	N/A	Describes how the institution's technology and security support the current and planned business operations; and	Functional	Subset Of	Cybersecurity & Data Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.	10	
609.935(e)	N/A	Reviews internal and external technology factors likely to affect the institution during the planning period	Functional	Subset Of	Cybersecurity & Data Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.	10	
609.935(e)	N/A	Reviews internal and external technology factors likely to affect the institution during the planning period	Functional	Intersects With	Cybersecurity & Data Protection Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
609.935(e)	N/A	Reviews internal and external technology factors likely to affect the institution during the planning period	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and data protection that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
609.935(e)	N/A	Reviews internal and external technology factors likely to affect the institution during the planning period	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	8	
609.945	Records retention.	Records stored electronically must be accurate, accessible, and reproducible for later reference.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
609.945	Records retention.	Records stored electronically must be accurate, accessible, and reproducible for later reference.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	8	