Farm Credit Administration (FCA) Cyber Risk Management Final Rule: Resource and Tandem Mapping

Introduction

On December 11, 2023, the Farm Credit Administration published their final rule over Cyber Risk Management (12 CFR Part 609) in the Federal Register. The rule is effective January 1, 2025. The rule requires farm credit institutions to implement a comprehensive, written cyber risk management program.

This resource is for information purposes only. It serves to provide Tandem's commentary on the final rule. You may use this resource to assist in your understanding of the regulation, but you should interpret the regulation, as appropriate, for your institution.

This resource also serves to identify areas in Tandem where topics from the final rule are addressed and does not guarantee that an institution using Tandem achieves the requirements.

About Tandem: Tandem is a tool designed to assist with compliance goals and improve cybersecurity through the development of a cyber risk management program. There are multiple Tandem products referenced in this mapping which can help address the requirements of the updated standards. These products include Risk Assessment, Policies, Vendor Management, Audit Management, Phishing, and Incident Management.

If you do not have access to the Tandem products referenced by this mapping, but would like to learn more, contact us at info@tandem.app or on our website, Tandem.App/Contact.

Section	Section Text	Tandem Commentary	Tandem Mapping
Subpart A – General Rules			
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.	This is a high-level overview, providing a lens through which farm credit institutions should view the rule.	Details on how Tandem addresses the final rule's requirements will be provided in applicable sections.
Subpart B – Standards for Boards and Management			
609.930 – Cyber risk management.			
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.	The FCA's definition of cyber risk management program overlaps with and expands on concepts traditionally addressed in an information security program, as required by GLBA. It requires institutions to protect "current, former, and potential customer and employee information."	Tandem is a suite of products designed to help financial institutions create a comprehensive, written cyber risk management program. Learn more at Tandem.App.
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: 1. 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; **2.** Oversee the development, implementation, and maintenance of the institution's cyber risk program; and **3.** Determine necessary expertise for executing the cyber risk management plan and, where practical, delegate day-to-day responsibilities to management and employees.	The board is required to 1) approve the program, 2) govern the program, and 3) ensure institution personnel are capable of implementing the program.	**Tandem Resources** • Annual Report to the Board • Information Security Program

609.930(c)	**Cyber risk program.** Each institution's cyber risk program must, at a minimum:		
609.930(c)(1)	Include an annual risk assessment of the internal and external factors likely to affect the institution. The risk assessment, at a minimum, must: i. 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 ii. Assess the sufficiency of policies, procedures, internal controls, and other practices in place to mitigate risks.	Institutions are required to perform a risk assessment that is virtually identical to a GLBA risk assessment. Learn more about this process on our blog: What is a GLBA Risk Assessment?	Use Tandem Risk Assessment to create risk assessments.
609.930(c)(2)	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.	Institutions are required to identify, prioritize, and remediate vulnerabilities in a "timely" manner. The term "timely" is left up to the institution's judgment.	Use Tandem Audit Management to document and track remediation status of vulnerabilities.
609.930(c)(3)	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:	Institutions are required to create an incident response plan and update it at least annually. Learn more about this process on our blog: The Six Phases of an Effective Incident Response Plan	Use Tandem Incident Management to create an incident response plan.
609.930(c)(3)(i)	Assessing the nature and scope of an incident, and identifying what information systems and types of information have been accessed or misused;	Institutions are required to perform incident analysis.	**Tandem Incident Management** • Incident Handling Process: Analysis • Action Plans
609.930(c)(3)(ii)	Acting to contain the incident while preserving records and other evidence;	Institutions are required to contain incidents carefully.	**Tandem Incident Management** • Incident Handling Process: Containment • Action Plans • Additional Documentation: Evidence

609.930(c)(3)(iii)	Resuming business activities during intrusion response;	Institutions are required to have a business continuity plan (BCP).	Use Tandem Business Continuity Plan to create business resumption and resilience plans. **Tandem Incident Management** • Incident Handling Process: Recovery • Action Plans
609.930(c)(3)(iv)	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;	Institutions are required to notify the board of specific incidents.	**Tandem Incident Management** • Additional Documentation: Internal Communication
609.930(c)(3)(v)	Notifying FCA as soon as possible or no later than 36 hours after the institution determines that an incident has occurred; and	Institutions are required to notify the FCA of incidents within 36 hours of determining the incident occurred. The FCA defines the types of incidents to be reported in their Informational Memorandum on Reporting Security Incidents and Business Continuity Events to FCA, dated June 27, 2017.	**Tandem Incident Management** • Additional Documentation: Third-Party Communication
609.930(c)(3)(vi)	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.	Institutions are required to notify customers, employees, and “known visitors to your website,” when an incident affects them. The FCA intentionally did not define these terms and expects each institution to “determine and document what these terms mean,” noting that “all confidential information related to ‘former, current, or potential customers and employees and known visitors to a website’ must be protected.”	**Tandem Incident Management** • Additional Documentation: Customer Communication

609.930(c)(4)	Describe the plan to train employees, vendors, contractors, and the institution board to implement the institution's cyber risk program.	Institutions are required to train – or – validate training is conducted for employees, vendors, contractors, and the board. The FCA's commentary states, "if an institution does not provide training, the institution must describe its plan and state why and what actions it is taking to mitigate the risk of not having institution-provided training. […] As to vendors, System institutions should be able to confirm, either contractually or otherwise, that vendors have some acceptable level of training."	Use the **Tandem Training** tool to provide cybersecurity awareness education. This tool is a feature of Tandem Phishing, Tandem Policies, and Tandem Incident Management. **Tandem Policies** • Security Awareness Training Policy **Tandem Vendor Management** • *Select Vendor > Documents*
609.930(c)(5)	Include policies for vendor management and oversight. Each institution, at a minimum, must:	Institutions are required to have a vendor management policy. Learn more about this process in our blog: What is Vendor Management?	**Tandem Vendor Management** **Tandem Policies** • Vendor Management Policy
609.930(c)(5)(i)	Exercise appropriate due diligence in selecting vendors;	Institutions are required to perform due diligence in selection.	**Tandem Vendor Management** • *Select Vendor > Documents* • Document Types • Review Templates
609.930(c)(5)(ii)	Negotiate contract provisions, when feasible, that facilitate effective risk management and oversight and specify the expectations and obligations of both parties;	Institutions are required to negotiate favorable and clear contracts.	**Tandem Vendor Management** • *Select Vendor > Contracts* • Review Templates: Contract Review
609.930(c)(5)(iii)	Conduct a vendor risk assessment on all vendors; and	Institutions are required to conduct vendor risk assessments.	**Tandem Vendor Management** • *Select Vendor > Services > Risk Assessment* • Risk Categories
609.930(c)(5)(iv)	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.	Institutions are required to ensure their vendors have adequate security testing performed (e.g., audits, penetration tests, vulnerability assessments, etc.).	**Tandem Vendor Management** • Document Types: Security Testing • Document Types: SOC Report • Review Template: Security Testing • Review Template: SOC Report

609.930(c)(6)	Maintain robust internal controls by regularly testing the key controls, systems, and procedures of the cyber risk management program.	Institutions are required to have “regular” security testing of their own controls.	Use Tandem Audit Management to track the institution’s assurance and testing process, as well as track remediation efforts.
609.930(c)(6)(i)	The frequency and nature of such tests are to be determined by the institution's risk assessment.	Institutions are required to perform an audit risk assessment. Learn more about this process in our blog: What is an IT Audit Risk Assessment?	Use Tandem Risk Assessment to create the audit risk assessment. Learn more in the Tandem Knowledge Base: IT Audit Risk Assessment. (You must have Tandem access to see this article.)
609.930(c)(6)(ii)	Tests must be conducted or reviewed by independent third parties or staff independent of those who develop or maintain the cyber risk management program.	Institutions are required to have independent validation. The same person implementing the program should not be the same person verifying it works.	Tandem’s sister company, CoNetrix Security, specializes in providing independent IT audit, penetration testing, and vulnerability assessment services to financial institutions.
609.930(c)(6)(iii)	Internal systems and controls must provide reasonable assurances that System institutions will prevent, detect, and remediate material deficiencies on a timely basis.	Institutions are required to do what is in their power to prevent, detect, and correct material control deficiencies. The FCA commentary says “material” in this context means *not* small or *de minimis* deficiencies.	Use Tandem Audit Management to track the institution’s assurance and testing process, as well as track remediation efforts.

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.	Institutions are required to consider privacy in the program.	Security and privacy controls often overlap. As such, the Tandem features described in this mapping can also be used to help protect privacy. Additional features related to privacy could include the following.
			
			Tandem Policies
			• Access Control Policy
			• Data Management Policy
			
			Tandem Risk Assessment
			• Data Types & Information Assets
			• Controls
			  • Least Privilege Access
			  • Logical Access Controls
			  • Physical Access Controls
			  • Separation of Duties

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.	Institutions are required to report to the board at least quarterly.	**Tandem Resources** • Annual Report to the Board Template
609.935 – Business planning.			
609.935	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: a. Describes the institution's intended technology goals, performance measures, and objectives; b. Details the technology budget; c. Identifies and assesses the adequacy of the institution's entire cyber risk management program, including proposed technology changes; d. Describes how the institution's technology and security support the current and planned business operations; and e. Reviews internal and external technology factors likely to affect the institution during the planning period.	Institutions are required to create a technology plan that describes things like goals, performance measures, budgets, proposed changes, etc.	N/A – This process would be best completed outside the Tandem application as part of the institution's overall business plan.
609.945 – Records retention.			
609.945	Records stored electronically must be accurate, accessible, and reproducible for later reference.	Institutions are required to retain records in accordance with business requirements.	**Tandem Policies** • Data Management Policy