RESOURCE & TANDEM MAPPING

CISA Cybersecurity Measures

INTRODUCTION

On January 18, 2022, the Cybersecurity & Infrastructure Security Agency (CISA) released a document titled Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats. The document comes during a time of heightened geopolitical tensions which could negatively impact the financial sector, so it is important for financial institutions to review the document and ensure the recommendations are implemented.

This resource is for information purposes only. It serves to identify areas in Tandem where topics from the document are addressed and does not guarantee that an organization using Tandem achieves the expectations. You may use this resource to assist in your understanding of the recommended measures, but you should interpret the guidance, as appropriate, for your organization.

About Tandem: Tandem is a Governance, Risk, and Compliance (GRC) tool designed to work with financial institutions to assist with compliance goals and improve cybersecurity through the development of an information security program. There are multiple Tandem products referenced in this mapping which can help address the requirements of the updated standards. These products include Incident Management, Policies, Business Continuity Planning, Risk Assessment, Vendor Management, and Audit 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.

Tandem™

REDUCE THE LIKELIHOOD OF A DAMAGING CYBER INTRUSION

CISA CHECKLIST ITEM	TANDEM MAPPING
Validate that all remote access to the organization's network and privileged or administrative access requires multi-factor authentication.	**Policies** • Remote Access **Risk Assessment** • Control: Multifactor Authentication
Ensure that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA.	**Policies** • Security Testing • Software Patches & Updates
Confirm that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes.	**Policies** • Demilitarized Zone (DMZ) • Security Testing • System Hardening
If the organization is using cloud services, ensure that IT personnel have reviewed and implemented strong controls outlined in CISA's guidance.	**Policies** • Access Control • Cloud Computing • Employee Security Awareness Training • Malicious Software Protection • System Hardening • User Authentication • Vendor Management **Vendor Management** Use this product to gather and review third-party cloud service provider due diligence.
Sign up for CISA's free cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats.	**Audit Management** Use this product to track results of vulnerability scanning and ensure adequate remediation. **Policies** • Security Testing • Software Patches & Updates **Tandem Partners** For additional security testing services, check out our list of Tandem Partners.

TAKE STEPS TO QUICKLY DETECT A POTENTIAL INTRUSION

CISA CHECKLIST ITEM	TANDEM MAPPING
Ensure that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior. Enable logging in order to better investigate issues or events.	**Incident Management** • Incident Handling Process: Detection **Policies** • Network Monitoring and Log Management

Confirm that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated.	**Policies**
	• Malicious Software Protection
	
	Risk Assessment
	• Controls:
	  • Anti-Malware Software
	  • Intrusion Detection/Prevention System

If working with Ukrainian organizations, take extra care to monitor, inspect, and isolate traffic from those organizations; closely review access controls for that traffic.	**Policies**
	• Access Control
	• Demilitarized Zone (DMZ)
	• Intrusion Detection and Prevention
	
	Risk Assessment
	• Controls:
	  • Internal Network Monitoring
	  • Intrusion Detection/Prevention System
	  • Limit Local Administrator Access
	  • Logical Access Controls
	
	Note: While these policies and controls do not explicitly mention traffic from Ukrainian organizations, the concepts included would apply.

ENSURE THAT THE ORGANIZATION IS PREPARED TO RESPOND IF AN INTRUSION OCCURS

CISA CHECKLIST ITEM	TANDEM MAPPING
Designate a crisis-response team with main points of contact for a suspected cybersecurity incident and roles/responsibilities within the organization, including technology, communications, legal and business continuity.	**Incident Management** • Additional Documentation: Internal Communication • Committees/Teams: Incident Response Team • Handler Roles • Roles & Responsibilities **Policies** • Incident Management
Assure availability of key personnel; identify means to provide surge support for responding to an incident.	**Business Continuity Plan** • Cross Training Matrix • Emergency Checklists: Customer Communication Checklist • Preparedness Controls: Customer Communication Plan • Order of Succession **Incident Management** • Additional Documentation: Internal Communication • Roles & Responsibilities **Policies** • Incident Management • Vendor Management **Risk Assessment** • Threat: Loss of Key Personnel **Vendor Management** Use this product to track contracts and service level agreements (SLAs) with key third parties.
Conduct a tabletop exercise to ensure that all participants understand their roles during an incident.	**Business Continuity Plan & Incident Management** • Exercises & Tests • Scenarios

MAXIMIZE THE ORGANIZATION'S RESILIENCE TO A DESTRUCTIVE CYBER INCIDENT

CISA CHECKLIST ITEM	TANDEM MAPPING

Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyberattack; ensure that backups are isolated from network connections.	**Business Continuity Plan**
	• Backup Profiles
	
	Incident Management
	• Action Plans:
	  • Malicious Code
	  • Ransomware
	
	Policies
	• Data Backup
	
	Risk Assessment
	• Control: Data Backup
	• Threats:
	  • Exploitation by Cyber Attack
	  • Malicious Software
	  • Simultaneous Cyber Attack on Multiple Data Centers

If using industrial control systems or operational technology, conduct a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted.	**Business Continuity Plan** • Business Processes: Recovery Objectives • Preparedness Controls • Exercises & Tests • Scenarios