Cybersecurity Supervision Work Program

The Cybersecurity Supervision Work Program (CSW) is a component of the Office of the Comptroller of the Currency's (OCC) risk-based bank information technology (BIT) supervision process. The CSW is designed to provide examiners an effective approach to identify cybersecurity risks in supervised banks.[1] In distributing the CSW to examiners, the OCC sets no new regulatory expectations.

In addition, the CSW is designed to align with the National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF).[2] This alignment provides examiners with a common framework and terminology in discussions with bank management. The CSW is structured according to the five NIST-CSF functions—Identify, Protect, Detect, Respond, and Recover—and the related categories and subcategories. The CSW does not include NIST-CSF subcategories that are addressed as part of other examination programs or subcategories that do not apply to the OCC bank supervision process. The OCC developed an additional function, Specialty Areas, to address areas of risk that may be part of OCC cybersecurity assessments, where applicable.

This attachment to OCC Bulletin 2023-22, "Cybersecurity: Cybersecurity Supervision Work Program," summarizes the CSW's high-level objectives and the corresponding categories and subcategories. Examiners use the relevant procedures from the CSW to supplement procedures contained in the "Community Bank Supervision," "Large Bank Supervision," and "Federal Branches and Agencies Supervision" booklets of the *Comptroller's Handbook*, related supervisory guidance, and the *Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook* booklets.

The OCC continues to encourage, but does not require, the use of standardized approaches to assess and improve cybersecurity preparedness. Banks may choose from a variety of standardized tools and frameworks available.[3] The CSW Overview page on www.occ.gov links to the CSW References page, which provides cross-references that map the CSW procedures to existing supervisory guidance and industry cybersecurity frameworks. These include the FFIEC Cybersecurity Assessment Tool, the Center for Internet Security's Critical Cybersecurity Controls, and the Cyber Risk Institute's Profile.

[1] "Banks" refers collectively to national banks, federal savings associations, covered savings associations, and federal branches and agencies of foreign banking organizations.

[2] Refer to the NIST-CSF at https://www.nist.gov/cyberframework.

[3] Refer to FFIEC press release titled "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness," August 28, 2019.

Function One: Identify (ID)

Develop an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities.

Categories

IT Asset Management (ID.AM): The objective of the IT Asset Management section is to evaluate the processes that enable identification, inventory, and maintenance of the hardware, software, data, and other IT-related assets that support bank operations. The procedures address processes and controls for data management, classification, mapping, and network and data flow diagrams. Examiners should refer to the "Architecture, Infrastructure, and Operations" booklet of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate the effectiveness of processes implemented to identify and maintain the asset inventory of all on-site and off-site system devices, hardware, and other system components.
- Evaluate the effectiveness of software inventory management processes to include end of support and end of life situations.
- Evaluate the effectiveness of the processes for developing, maintaining, and securing data flow diagrams.
- Assess the processes for identifying and maintaining an inventory of all external connections.
- Evaluate the effectiveness of the data management life cycle to include identification, analysis, storage, and disposal.
- Assess the adequacy of the data classification methodology to determine if data criticality and sensitivity are identified and maintained.

NIST-CSF References

- **ID.AM-1:** Physical devices and systems within the organization are inventoried.
- **ID.AM-2:** Software platforms and applications within the organization are inventoried.
- **ID.AM-3:** Organizational communication and data flows are mapped.
- **ID.AM-4:** External information systems are catalogued.
- **ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.
- **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, and partners) are established.

Business Environment (ID.BE): The objective of the Business Environment section is to evaluate the bank's role in the financial sector, understand key dependencies and assess whether the dependencies are understood, prioritized, and used to inform cybersecurity roles, responsibilities, risk management, and decisions. The procedures address the bank's role in critical infrastructure, evaluate critical dependencies, and consider how these evaluations inform the bank's cybersecurity resilience plans and capabilities. Examiners should refer to the

"Architecture, Infrastructure, and Operations" booklet of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate how management determines and communicates if the bank holds a critical or systemically important role in providing services to other entities in the financial sector.
- Evaluate how management determines and communicates the bank's role in the financial services sector of the U.S. critical infrastructure.
- Evaluate the effectiveness of processes that identify and maintain critical dependencies, such as power, telecommunications, network connectivity, and other critical infrastructures.
- Evaluate cybersecurity resilience planning and response capabilities to support delivery of critical services.

NIST-CSF References

- **ID.BE-1:** The organization's role in the supply chain is identified and communicated.
- **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated.
- **ID.BE-3**: Priorities for organizational mission, objectives, and activities are established and communicated.
- **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established.
- **ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, and normal operations).

Governance (ID.GV): The objective of the Governance section is to evaluate the organization's risk management processes and governance structure for managing cybersecurity risk. The procedures assess cybersecurity governance to include roles and responsibilities and compliance with rules and regulations, such as requirements to maintain an information security program to safeguard customer information and incident notification. The procedures also assess the bank's assurance and testing processes including IT audit and penetration testing. Examiners should refer to the "Audit," "Management," and "Architecture, Infrastructure, and Operations" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Review management and staff roles and responsibilities to determine whether they address cybersecurity risk management processes and procedures.
- Evaluate the processes' effectiveness for maintaining continued compliance with applicable rules and regulations.
- Assess the effectiveness of cybersecurity risk management processes.
- Review and evaluate assurance and testing processes to determine whether cybersecurity controls are in place and working effectively to mitigate identified security risks.
- Assess the adequacy of scope, frequency, and effectiveness of penetration testing.

NIST-CSF References

- **ID.GV-1:** Organizational cybersecurity policy is established and communicated.
- **ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.
- **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
- **ID.GV-4:** Governance and risk management processes address cybersecurity risks.

Risk Assessment (ID.RA): The objective of the Risk Assessment section is to evaluate the bank's threat and vulnerability identification process. Procedures evaluate threat intelligence sources and analysis. Analysis includes threat prioritization, likelihood of occurrence, and severity of impact. Examiners determine whether the risk assessment evaluates potential business disruptions and their impact to the bank, assets, and personnel. Examiners also determine whether management's response or action taken to identified risk is acceptable. Examiners should refer to the "Information Security" booklet of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate the effectiveness of threat intelligence collection from external sources.
- Evaluate the cybersecurity risk assessment process to assess whether threats, vulnerabilities, likelihoods, and impacts are used to determine business impacts and overall risk.
- Assess the effectiveness of management's prioritization and response to identified risks to include consideration of cybersecurity insurance.

NIST-CSF References

- **ID.RA-1**: Asset vulnerabilities are identified and documented.
- **ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources.
- **ID.RA-3:** Threats, both internal and external, are identified and documented.
- **ID.RA-4:** Potential business impacts and likelihoods are identified.
- **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
- **ID.RA-6:** Risk responses are identified and prioritized.

Risk Management Strategy (ID.RM): The objective of the Risk Management Strategy section is to evaluate the bank management's strategic decisions and responses to ongoing and emerging cybersecurity threats. The procedures evaluate cybersecurity risk management as a means to inform strategic decisions, risk appetite, and risk tolerance. Examiners should refer to the "Information Security" booklet of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate, as part of cybersecurity risk management, the effectiveness of strategic decisions with regard to business constraints, business priorities, and risk tolerances.

- Evaluate the effectiveness of processes used to determine risk appetite and risk tolerance for cybersecurity.
- Determine whether management considers and incorporates the bank's role as part of critical infrastructure when establishing risk appetite or risk tolerances.

NIST-CSF References

- **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.
- **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed.
- **ID.RM-3:** The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.

Supply Chain Risk Management (ID.SC): The objective of the Supply Chain Risk Management section is to evaluate priorities, constraints, risk tolerances, and assumptions that support risk decisions associated with managing supply chain risk. This procedure addresses supply chain risk from a cybersecurity perspective and is intended to supplement examination procedures associated with the interagency guidance on third-party relationships.[4] Examiners should evaluate how cybersecurity risk is integrated with, or considered as part of, overall third-party risk management. Examiners should refer to the "Information Security" and "Architecture, Infrastructure, and Operations" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate how management incorporates cybersecurity and supply chain risk assessment into their third-party risk management processes.

NIST-CSF References

- **ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.
- **ID.SC-2:** Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.
- **ID.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.
- **ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
- **ID.SC-5:** Response and recovery planning and testing are conducted with suppliers and third-party providers.

[4] Refer to OCC Bulletin 2023-17, "Third-Party Relationships: Interagency Guidance on Risk Management," and OCC Bulletin 2021-40, "Third-Party Relationships: Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks."

Function Two: Protect (PR)

Outline appropriate safeguards to ensure delivery of critical infrastructure services.

Categories

Identity Management, Authentication, and Access Control (PR.AC): The objective of the Identity Management, Authentication, and Access Control section is to evaluate the implementation and administration of logical and physical access controls in place to safeguard the bank's information assets, to include data and technology. The procedures evaluate access management and authentication practices to include user identification and verification, remote and privileged users, system authentication, and network segmentation. Examiners should refer to the "Information Security" booklet of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate the effectiveness of the access management processes to implement and administer logical and physical access controls. This includes assessing authentication controls and use of multifactor authentication or similarly strong controls.
- Evaluate the effectiveness of processes to manage remote access.
- Evaluate the effectiveness of processes to manage accounts with privileged access.
- Evaluate the effectiveness of processes governing network segmentation, including planning and implementation.
- Assess the adequacy of identity verification and management processes.
- Evaluate the adequacy of processes to manage user authentication practices.
- Evaluate the adequacy of processes to manage system to system authentication.

NIST-CSF References

- **PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
- **PR.AC-2:** Physical access to assets is managed and protected.
- **PR.AC-3:** Remote access is managed.
- **PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
- **PR.AC-5:** Network integrity is protected (e.g., network segregation and network segmentation).
- **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions.
- **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor and multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).

Awareness and Training (PR.AT): The objective of the Awareness and Training section is to assess whether system users are trained to carry out information security responsibilities in a manner consistent with bank policies, procedures, and agreements or contracts. The procedure addresses training programs to determine whether they strengthen compliance with cybersecurity and acceptable use policies and promote a strong security culture. Examiners should refer to the "Information Security" and "Management" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate the adequacy of information security training and awareness programs.

NIST-CSF References

- **PR.AT-1:** All users are informed and trained.
- **PR.AT-2:** Privileged users understand their roles and responsibilities.
- **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, and partners) understand their roles and responsibilities.
- **PR.AT-4:** Senior executives understand their roles and responsibilities.
- **PR.AT-5:** Physical and cybersecurity personnel understand their roles and responsibilities.

Data Security (PR.DS): The objective of the Data Security section is to evaluate the processes in place to protect the confidentiality, integrity, and availability of data and to determine whether data is managed in accordance with the bank's security policies and risk appetite. The procedures address the adequacy of protections in place for data at rest and in-transit to include consideration for encryption practices, key management, electronic media, mobile device management, data loss protection, and capacity and hardware integrity. Examiners should refer to the "Information Security" booklet of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess the adequacy of processes to plan and implement effective encryption practices for data at rest and data in-transit.
- Assess the adequacy of cryptographic key and certificate management processes.
- Evaluate the effectiveness of processes to manage electronic media storage, transit, sanitization, and disposal.
- Assess the adequacy of processes to manage mobile devices used for critical functions or contain confidential data.
- Evaluate the effectiveness of processes to minimize or prevent the risk of data loss.
- Assess the adequacy of processes to manage system capacity.
- Assess the adequacy of processes that identify and manage hardware integrity.

NIST-CSF References

- **PR.DS-1:** Data-at-rest is protected.
- **PR.DS-2:** Data-in-transit is protected.
- **PR.DS-4:** Adequate capacity to ensure availability is maintained.
- **PR.DS-5:** Protections against data leaks are implemented.
- **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity.
- **PR.DS-7:** The development and testing environment(s) are separate from the production environment.

- **PR.DS-8:** Integrity checking mechanisms are used to verify hardware integrity.

Information Protection Processes and Procedures (PR.IP): The objective of the Information Protection Processes and Procedures section is to assess whether security policies, processes, and procedures are maintained and used to manage and protect information systems and assets. The procedures address how management defines and manages security control baselines (e.g., hardening practices) and addresses governance practices, including data backup, and response plan governance, execution, and testing. Examiners should refer to the "Information Security," "Management," "Business Continuity Management," and "Architecture, Infrastructure, and Operations" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess the adequacy of processes to identify and manage security baselines.
- Assess the adequacy of backup strategies and processes to protect data from physical and cyber threats.
- Assess the adequacy of governance and oversight of response plans supporting cybersecurity protection.
- Assess the adequacy of cybersecurity incident response and recovery plan testing.

NIST-CSF References

- **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality).
- **PR.IP-2:** A System Development Life Cycle to manage systems is implemented.
- **PR.IP-3:** Configuration change control processes are in place.
- **PR.IP-4:** Backups of information are conducted, maintained, and tested.
- **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met.
- **PR.IP-6:** Data is destroyed according to policy.
- **PR.IP-7:** Protection processes are improved.
- **PR.IP-8:** Effectiveness of protection technologies is shared.
- **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
- **PR.IP-10:** Response and recovery plans are tested.
- **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning and personnel screening).
- **PR.IP-12:** A vulnerability management plan is developed and implemented.

Maintenance (PR.MA): The objective of the Maintenance section is to assess whether the bank has adequate processes and tools to maintain information systems and whether practices are consistent with policies and procedures. The procedure addresses asset maintenance practices and tools from a cybersecurity perspective. Examiners should refer to the "Architecture, Infrastructure, and Operations" booklet of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess the adequacy of processes and tools to maintain IT assets.

NIST-CSF References

- **PR.MA-1:** Maintenance and repair of organizational assets are performed and logged with approved and controlled tools.
- **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.

Protective Technology (PR.PT): The objective of the Protective Technology section is to evaluate technical security solutions that enable the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. The procedures address controls such as system logging practices, portable devices, removable media and disposal, the concept of least function configuration, and fail secure practices. Examiners should refer to the "Information Security," "Management," and "Architecture, Infrastructure, and Operations" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess the adequacy of processes to manage audit and system logs.
- Evaluate the processes to manage removable media and portable devices.
- Assess the adequacy of processes to manage data disposal and device sanitization.
- Assess the adequacy of processes for configuring systems and components based on the principle of least functionality.
- Assess the adequacy of network and communications resiliency.
- Assess the processes to implement fail secure controls.

NIST-CSF References

- **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
- **PR.PT-2:** Removable media are protected and their use restricted according to policy.
- **PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
- **PR.PT-4:** Communications and control networks are protected.
- **PR.PT-5:** Mechanisms (e.g., failsafe, load balancing, and hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

Function Three: Detect (DE)

Define the appropriate activities to identify the occurrence of a cybersecurity event.

Categories

Anomalies and Events (DE.AE): The objective of the Anomalies and Events section is to evaluate whether processes and controls to detect anomalous activity are timely and effective. The procedures address network performance baselines, network monitoring activities, configuration management, threat intelligence, and event management. Examiners should refer to the "Information Security" and "Architecture, Infrastructure, and Operations" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate the effectiveness of the process for establishing and managing baseline network activity and normal internal and external data flows for users and systems, including those with third parties.
- Assess the adequacy of processes that monitor network activities and identify and alert for anomalous activity and traffic patterns.
- Evaluate the effectiveness of processes used to manage system configuration baselines and to detect unauthorized changes from the baseline configuration.
- Evaluate the effectiveness of processes that identify and analyze events.
- Assess the adequacy of processes that define, manage, and adjust alert parameters for detecting and notifying management of events/incidents.
- Evaluate the effectiveness of log collection and log data aggregation processes to determine whether event data are relevant, accurate, and complete.
- Evaluate the effectiveness of the processes for correlating threat intelligence with internal event data analysis.
- Assess the adequacy of processes for analyzing the impact from active event(s).
- Evaluate the effectiveness of the process used to establish alert thresholds to determine when an event is designated as an incident.

NIST-CSF References

- **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.
- **DE.AE-2:** Detected events are analyzed to understand attack targets and methods.
- **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors.
- **DE.AE-4:** Impact of events is determined.
- **DE.AE-5:** Incident alert thresholds are established.

Security Continuous Monitoring (DE.CM): The objective of the Security Continuous Monitoring section is to evaluate the effectiveness of processes and controls for monitoring information systems and assets to help identify anomalous events. The procedures address network monitoring, malware and malicious code, unauthorized assets and code, and vulnerability scanning. For this function, scanning is part of overall vulnerability management, whereas in the "Respond" function, scanning identifies additional vulnerabilities detected during incident mitigation. Examiners should refer to the "Management" and "Information Security" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess the adequacy of processes to monitor the network for events (e.g., unauthorized personnel and third-party connections).
- Assess the effectiveness of the risk management processes that determine the scope and type of implemented monitoring solutions.
- Assess effectiveness of controls over the physical facility and technology assets.
- Evaluate the effectiveness of application-level controls that identify, measure, monitor, manage, and report anomalous activities.
- Evaluate the effectiveness of processes and controls to detect unauthorized mobile code.
- Evaluate the adequacy of processes and the effectiveness of detection tools to identify and monitor for shadow IT.
- Evaluate the adequacy of the scope, frequency, and effectiveness of the vulnerability scanning process.

NIST-CSF References

- **DE.CM-1:** The network is monitored to detect potential cybersecurity events.
- **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events.
- **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events.
- **DE.CM-4:** Malicious code is detected.
- **DE.CM-5:** Unauthorized mobile code is detected.
- **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events.
- **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed.
- **DE.CM-8:** Vulnerability scans are performed.

Detection Processes DE.(DP): The objective of the Detection Processes section is to assess whether event detection practices are timely and effective. The procedures address detection processes that identify anomalous events, including the timeliness of event detection and the testing of detection processes. Examiners should refer to "Business Continuity Management" and "Information Security" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess the effectiveness of detection processes, including planning and implementation, personnel, and communication of event information.
- Assess the adequacy of detection process testing.

NIST-CSF References

- **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability.
- **DE.DP-2:** Detection activities comply with all applicable requirements.
- **DE.DP-3:** Detection processes are tested.
- **DE.DP-4:** Event detection information is communicated.
- **DE.DP-5:** Detection processes are continuously improved.

Function Four: Respond (RS)

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident and support the ability to contain the impact of a potential cybersecurity incident.

Categories

Response Planning (RS.RP): The objective of the Response Planning section is to assess whether response plans are executed in a manner that enable timely response to detected cybersecurity events. This commonly involves reviewing bank responses to actual events or test results. Examiners should refer to OCC Bulletin 2021-55, "Computer-Security Incident Notification: Final Rule," and the "Business Continuity Management" and "Information Security" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess effectiveness of processes related to execution of the cybersecurity incident response plan.

NIST-CSF References

- **RS.RP-1:** Response plan is executed during or after an incident.

Communications (RS.CO): The objective of the Communications section is to assess the adequacy of response activities with internal and external stakeholders. The procedures address information sharing strategies, stakeholder coordination, and sector-wide information sharing. Examiners should refer to the "Information Security" and "Business Continuity Management" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess the appropriateness of strategy and practices to share information with affected staff, industry groups (e.g., Financial Services Information Sharing and Analysis Center (FS-ISAC)), financial sector, regulators, and peers.
- Assess the adequacy of internal and external stakeholder coordination in accordance with the response plan.
- Evaluate information sharing arrangements to assess the effectiveness of sharing threats and countermeasures with other external stakeholders in order to support sector-wide situational awareness and response to incidents.

NIST-CSF References

- **RS.CO-1:** Personnel know their roles and order of operations when a response is needed.
- **RS.CO-2:** Incidents are reported consistent with established criteria.
- **RS.CO-3:** Information is shared consistent with response plans.
- **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans.
- **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.

Analysis (RS.AN): The objective of the Analysis section is to assess the adequacy of processes that escalate events to formal incident status and to evaluate incident response processes. The procedures address the adequacy of event investigation, incident impact analysis, forensic investigation, incident prioritization, and processes that identify and manage the vulnerabilities contributing to the incident. Examiners should refer to the "Business Continuity Management" and "Information Security" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess the adequacy of the processes to investigate event notifications.
- Evaluate the effectiveness of processes that analyze the impact of an incident.
- Assess the adequacy of forensic investigation processes, to include planning, scope, and timeliness.
- Assess the adequacy of criteria to categorize and prioritize incidents.
- Evaluate the effectiveness of processes that receive, analyze, and respond to vulnerabilities.

NIST-CSF References

- **RS.AN-1:** Notifications from detection systems are investigated.
- **RS.AN-2:** The impact of the incident is understood.
- **RS.AN-3:** Forensics are performed.
- **RS.AN-4:** Incidents are categorized consistent with response plans.
- **RS.AN-5:** Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).

Mitigation (RS.MI): The objective of the Mitigation section is to assess the effectiveness of response activities to prevent expansion of an incident or further contagion, mitigate its effects, and eradicate the incident. The procedures address incident containment and mitigation of contributing and any additional vulnerabilities identified as part of response activities. Examiners should refer to the "Information Security" and "Management" booklets of the *FFIEC IT Examination Handbook.* In this section, examiners will:

- Assess the adequacy of incident containment processes to minimize damage from the effects of an incident.
- Assess the adequacy of incident mitigation processes as defined in the response plan or evidenced during actual incidents.
- Assess the adequacy of processes to respond to additional vulnerabilities identified during mitigation.

NIST-CSF References

- **RS.MI-1:** Incidents are contained.
- **RS.MI-2:** Incidents are mitigated.
- **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks.

Improvements (RS.IM): The objective of the Improvements section is to assess whether incident response activities are improved by incorporating lessons learned from actual or simulated response activities. The procedure addresses how management incorporates post incident lessons learned to improve response plans. Examiners should refer to the "Information Security," "Management," and "Architecture, Infrastructure, and Operations" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess adequacy of processes that analyze and incorporate lessons learned to the Incident Response Plan.

NIST-CSF References

- **RS.IM-1:** Response plans incorporate lessons learned.
- **RS.IM-2:** Response strategies are updated.

Function Five: Recover (RC)

Identify appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Categories

Recovery Planning (RC.RP): The objective of the Recovery Planning section is to evaluate recovery processes and procedures that enable timely restoration of systems or assets affected by cybersecurity events. The procedure addresses the adequacy of restoration capabilities and processes. This assessment may involve review of actual incidents or testing scenarios. Examiners should refer to the "Business Continuity Management" and "Information Security" booklets of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate the effectiveness of incident recovery plans and restoration processes, including recovery plan testing.

NIST-CSF Reference

- **RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident.

Recovery Improvements (RC.IM): The objective of the Improvements section is to assess whether lessons learned are being considered and used to improve recovery plans and processes. The procedure addresses how management uses threat intelligence and lessons learned to inform recovery and restoration activities. Examiners should refer to the "Business Continuity Management" booklet of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Assess if recovery plans and tests are updated to include current threat intelligence, recognize lessons learned, and address issues identified during actual incidents or tests.

NIST-CSF References

- **RC.IM-1:** Recovery plans incorporate lessons learned.
- **RC.IM-2:** Recovery strategies are updated.

Recovery Communications (RC.CO): The objective of the Communications section is to evaluate how the bank communicates recovery activities. The procedure addresses internal and external communications that report the incident recovery status and recovery actions to internal and external stakeholders. Examiners should refer to the "Business Continuity Management" booklet of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate the effectiveness of communication to internal and external stakeholders regarding recovery activities.

NIST-CSF References

- **RC.CO-1:** Public relations are managed.
- **RC.CO-2:** Reputation is repaired after an incident.
- **RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams.

Specialty Areas (SA)

The OCC developed an additional function called Specialty Areas to address additional areas of risk that may be part of OCC cybersecurity assessments, where applicable. Specialty Area procedures will be applied during examinations based on bank operations and risk-based supervision strategy.

Secure Software Development (SA.SD): The Secure Software Development section is an examination area developed specifically by the OCC to evaluate the adequacy of system development life cycle and secure coding. The objective of the Secure Software Development section is to evaluate whether secure coding and development practices are applied when bank management engages in internal software development activities. The procedures address fundamental software development processes and secure coding standards. The procedures also address testing environment security and protecting nonpublic information. Examiners should refer to the “Development and Acquisition” booklet of the *FFIEC IT Examination Handbook*. In this section, examiners will:

- Evaluate the effectiveness of processes governing in-house software development to ensure cybersecurity is considered at all phases.
- Evaluate the effectiveness of processes and standards that enable secure coding practices.
- Evaluate the effectiveness of processes to review code for vulnerabilities and security weaknesses prior to release. Consider the criticality or sensitivity of the data.
- Evaluate the effectiveness of controls in place to protect nonpublic personal information in test environments.
- Evaluate the effectiveness of processes in place to protect and restrict access to source code.
- Evaluate the effectiveness of processes associated with implementing emergency changes to ensure cybersecurity is considered.
- Assess the adequacy of tools or practices to identify and remediate code vulnerabilities or code that is noncompliant with internal security standards.