Simplify Compliance for FFIEC-NCUA with the AWN CyberSOC™ Service

AWN CyberSOC™ Service

- Expert managed threat detection and response
- Dedicated security expertise for your IT team
- 24/7 monitoring with unlimited log sources

Benefits

- Simplifies FFIEC/NCUA compliance with customized reporting
- Monitors access to information systems and nonpublic information both on-premises and in the cloud
- Provides near real-time alerts on critical security incidents

The Federal Financial Institutions Examination Council (FFIEC) is the inter-agency body of the United States government that prescribes uniform principles, standards and report forms for the federal examination of financial institutions. It is empowered by various entities including the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the Consumer Financial Protection Bureau (CPFB).

The FFIEC makes recommendations to promote uniformity in the supervision of financial institutions. Regulated financial institutions must comply with the guidelines of FFIEC consistent with the Gramm-Leach-Bliley Act of 1999 (GLBA). FFIEC documented the necessary controls for compliance in the “FFIEC Information Security Handbook” and subsequently provided a cybersecurity assessment tool to help financial institutions improve their cybersecurity postures.

Complying with FFIEC/NCUA guidance can challenge financial institutions that have limited resources, but Arctic Wolf helps organizations meet many of the FFIEC/NCUA requirements with a turnkey SOC-as-a-service solution—the AWN CyberSOC. This document maps the specific control requirements in the FFEIC Information Security handbook to the AWN CyberSOC.

Who Is Affected

The FFIEC/NCUA guidance and supervision affects federally supervised financial institutions, their holding companies, and the nonfinancial institution subsidiaries of those institutions and holding companies. This includes banks insured by the FDIC, credit unions supervised by the NCUA, national banks and their subsidiaries supervised by the OCC.

Mapping FFIEC/NCUA to the AWN CyberSOC™ Service

The table below maps the FFIEC Cybersecurity Assessment Tool version 1.1 requirements in the FFIEC Information Technology (IT) Examination Handbook booklet on Information Security, and functionality provided by the AWN CyberSOC.

FFIEC/NCUA Control Objective	FFIEC/NCUA Control Activity (abbreviated)	AWN CyberSOC™ Service Capability
Domain 1 – Cyber Risk Management and Oversight		
Governance/Oversight: Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually.	Source: FFIEC Information Technology Examination Handbook on Information Security (IS).III.C:pg50: The sharing of attack data through organizations, such as FS-ISAC, may help industry institutions better assess and respond to current attacks. Management should consider information sharing as a part of its strategy.	AWN CyberSOC provides visibility into a financial institution's security posture through the Arctic Wolf customer portal dashboard and executive summary reports.
Governance/Strategy-Policies: The institution has board-approved policies commensurate with its risk and complexity that address information security.	Source: IS.I:pg4: Management also should establish appropriate policies, standards, and procedures to support the information security program.	AWN CyberSOC provides procedures to monitor a financial institution's environment and detect and respond to cybersecurity threats.
Governance/Strategy-Policies: The institution has policies commensurate with its risk and complexity that address the concepts of incident response and resilience.	Source: IS.II.C.21:pg43: Management should establish and maintain policies that address incident response and resilience and test incident scenarios.	AWN CyberSOC identifies the highest priority security incidents that IT organizations must rapidly respond to. Arctic Wolf offers incident response (IR) simulations to test a firm's IR escalation processes.
Risk Management/Risk Assessment: A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats and the sufficiency of policies, procedures, and customer information systems.	Source: IS.I.B:pg4: Management should provide an annual report to the board covering its risk assessment process, including threat identification and assessment.	Arctic Wolf's Concierge Security™ team (CST) conducts regular external vulnerability scans. The Arctic Wolf CST helps address a firm's most critical weaknesses and helps implement improvements.
Risk Management/Risk Assessment: The risk assessment identifies internet-based systems and high-risk transactions that warrant additional authentication controls.	Source: IS.I.B:pg4: Management should provide an annual report to the board covering its risk assessment process, including threat identification and assessment.	Arctic Wolf performs regular vulnerability scanning to help identify vulnerabilities in internet-facing systems and Active Directory group modifications for default admin level groups as well as customized groups that could grant access to systems in this category. Vulnerability reports demonstrate improvement of overall security posture of IT infrastructure.

FFIEC/NCUA Control Objective	FFIEC/NCUA Control Activity (abbreviated)	AWN CyberSOC™ Service Capability
Risk Management/Risk Assessment: The risk assessment is updated to address new technologies, products, services, and connections before deployment.	Source: IS.II.A:pg7: The institution should factor in external events affecting IT and the institution's ability to meet its operating objectives into the risk identification process.	The AWN CyberSOC service helps to increase risk maturity and reduce the risk impact by performing detection/response and by providing feedback on enhancing overall security posture.
Risk Management/Audit: Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance).	Source: FFIEC Information Technology Examination Handbook on Operations (OPS).B.29: Operations management should periodically review all logs. IS.II.C.22:pg43: Logging practices should be reviewed periodically by an independent party.	AWN CyberSOC collects and manages log records from on-premises systems and cloud sources. Event collection aggregates and retains raw log records for the varying duration required by the financial institution (default is 90 days) if needed for forensics purposes.
Resources/Staffing: Processes are in place to identify additional expertise needed to improve information security defenses.	Source: IS.I.C:pg5:. Management should provide, and the board should oversee, adequate funding to develop, implement, and maintain a successful information security program.	Financial institution IT staff are augmented by Arctic Wolf's Concierge Security™ team's expertise in managed detection and response to better protect financial institution information and infrastructure.
Domain 2 – Threat Intelligence and Collaboration		
Threat Intelligence/Threat Intelligence and Information: Threat information is used to monitor threats and vulnerabilities.	Source: IS.III.A:pg47: Management should develop procedures for obtaining, monitoring, assessing, and responding to evolving threat and vulnerability information.	AWN CyberSOC includes subscriptions to the latest threat intelligence to monitor events such as virus signatures, malicious IPs/domains, emerging network threats, and geo-locations, which help identify current threats and vulnerabilities.
Threat Intelligence/Threat Intelligence and Information: Threat information is used to enhance internal risk management and controls.	Source: IS.III.A:pg48: Once a threat is identified and vulnerabilities are assessed, the significance of the threat should trigger an appropriate response and include remediation options. Design policies to deal with immediate and consequential threats expeditiously, while addressing less significant threats are as part of a broader risk management process.	Arctic Wolf continuously monitors on-premises systems and cloud resources and displays in a customer portal a rating of the financial institution's security posture, including vulnerability management status, outstanding security incidents and network activity.
Monitoring and Analyzing/ Monitoring and Analyzing: Audit log records and other security event logs are reviewed and retained in a secure manner.	Source: IS.II.C.22:pg44: Management should have effective log retention policies that address the significance of maintaining logs for incident response and analysis needs. … Additionally, logging practices should be reviewed periodically by an independent party to ensure appropriate log management. … Regardless of the method of log management, management should develop processes to collect, aggregate, analyze, and correlate security information.	AWN CyberSOC collects and manages log records from on premises systems and cloud sources. The event collection function aggregates and retains raw log records for the varying duration required by the financial institution (default is 90 days). The AWN CyberSOC™ service correlates activities to detect and respond to anomalies for on premises systems and cloud resources, detecting and responding to anomalies located via sophisticated filtering, correlation and threshold rules.

FFIEC/NCUA Control Objective	FFIEC/NCUA Control Activity (abbreviated)	AWN CyberSOC™ Service Capability
Monitoring and Analyzing/ Monitoring and Analyzing: Computer event logs are used for investigations once an event has occurred.	Source: IS.II.C.22:pg44: Log files are critical to successfully address security incidents and can potentially contain sensitive information. Security information and event management (SIEM) systems collect, aggregate, analyze, and correlate information from discrete systems and applications.	The AWN CyberSOC service uses human-assisted machine learning to accurately detect advanced threats and reduce false positives. It leverages a cloud-based SIEM that collects, aggregates, analyzes and correlates information, allowing the AWN Concierge Security™ team to investigate and resolve events as they occur.
Information Sharing/Information Sharing: Information security threats are gathered and shared with applicable internal employees.	Source: IS.II.D:pg45: Risk reporting produces reports that address threats, capabilities, vulnerabilities, and inherent risk changes. It also evaluates the management's response and resilience to those events.	The Arctic Wolf Concierge Security™ team (CST) is the primary contact to the AWN CyberSOC service. The Arctic Wolf CST escalates the security incidents to financial institution IT staff via trouble-tickets, or via phone. The AWN CyberSOC portal provides an overview of a firm's overall security posture, including a security incidents dashboard.
Domain 3 – Cybersecurity Controls		
Preventive Controls/Infrastructure Management: All ports are monitored.	Source IS.II.C.12:pg26: Port monitoring to identify unauthorized network connections.	The AWN CyberSOC scans for unauthorized services on internet-facing systems and flags suspicious ports.
Preventive Controls/Infrastructure Management: Up-to-date anti-virus and anti-malware tools are used.	Source: IS.II.C.12:pg26: Management should implement defense-in-depth to protect, detect, and respond to malware.	The Arctic Wolf CST can advise the financial institution's IT staff on the optimal anti-virus and anti-malware tools to use.
Detective Controls/Threat and Vulnerability Detection: Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network.	Source: ISIS.II.C.17:pg38: Management should perform appropriate tests (e.g., penetration tests, vulnerability assessments, and application security tests) before launching or making significant changes to external-facing applications.	The Arctic Wolf CST runs periodic scans of the financial institution's externally-exposed systems for vulnerabilities and continually monitors network traffic and log files for potential compromise.
Detective Controls/Threat and Vulnerability Detection: Anti-virus and anti-malware tools are used to detect attacks.	Source: IS.II.C.12:pg26: Management should implement defense-in-depth to protect, detect, and respond to malware.	The AWN CyberSOC service checks for known malware (example: ransomware) by monitoring incoming network traffic, and outgoing command-and-control traffic. AWN CyberSOC can also ingest malware alerts from endpoint protection platform (EPP) or endpoint detection and response (EDR) solutions.

FFIEC/NCUA Control Objective	FFIEC/NCUA Control Activity (abbreviated)	AWN CyberSOC™ Service Capability
Detective Controls/Threat and Vulnerability Detection: Firewall rules are audited or verified at least quarterly.	Source: IS.III:pg46: Security operations activities can include security software and device management (e.g., maintaining the signatures on signature-based devices and firewall rules).	Arctic Wolf provides advisory services to audit firewall configurations, network zoning, and segmentation architecture, and can recommend changes that ensure business-critical assets are adequately protected from both internal and external cyberattacks.
Detective Controls/Anomalous Activity Detection: The institution is able to detect anomalous activities through monitoring across the environment.	Source: IS.II.C.12:pg26: Management should implement defense-in-depth strategies to protect, detect, and respond to malware.	AWN CyberSOC continually monitors on-premises systems and cloud assets to detect anomalous activities.
Detective Controls/Anomalous Activity Detection: Logs of physical and/or logical access are reviewed following events.	Source: ISIII.C.22:pg44: Institutions maintain event logs to understand an incident or cyber event after it occurs. Monitoring event logs for anomalies and relating that information with other sources broadens the institution's ability to understand trends, react to threats, and improve stakeholder reports.	AWN CyberSOC retains log data and network flow data for on-premises systems as well as available log data from cloud services. Such logs are maintained for threat detection and for subsequent incident response to broaden an institution's ability to respond to cyber threats.
Detective Controls/Event Detection: Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.	Source: IS.Introduction:pg2: Management should be able to identify and characterize threats, assess risks, make decisions regarding the implementation of appropriate controls, and provide appropriate monitoring and reporting.	Arctic Wolf audits changes to Active Directory (AD), Group Policies, Exchange and file servers, and flags unauthorized actions. AWN monitors failed/successful logins/ logoffs and all password changes to prevent excessive help desk calls.
Detective Controls/Event Detection: Responsibilities for monitoring and reporting suspicious systems activity have been assigned.	Source: IS.III.B:pg48: Management should establish responsibility and authority of security personnel and system administrators for monitoring to address indicators of vulnerabilities, attacks, compromised systems, and suspicious users.	The Arctic Wolf CST functions as a seamless extention of a financial institution's IT team and monitors and reports on suspicious activity.
Domain 4 – External Dependency Management		
Relationship Management/ Ongoing Monitoring: Audits, assessments, and operational performance reports are obtained and reviewed regularly, validating security controls for critical third parties.	Source: IS.II.C.20:pg42: Management should oversee outsourced operations through an independent review of the third party's security via appropriate reports from audits and tests.	Arctic Wolf facilitates the development of financial institution policies and procedures related to security monitoring and incident response. The AWN CyberSOC service monitors third-party cloud applications including SaaS applications (Office 365, G Suite, Box, Salesforce) as well as IaaS platforms (AWS, Azure) to minimize third-party cybersecurity risk. As it relates to the AWN CyberSOC service, Arctic Wolf maintains written policies based on a risk assessment consistent with our SOC II Type 2 compliance certification. AWN has strict security policies in place to prevent unauthorized access to SOC tools. Log data is encrypted in transit and at rest.

FFIEC/NCUA Control Objective	FFIEC/NCUA Control Activity (abbreviated)	AWN CyberSOC™ Service Capability
Domain 5 – Cyber Incident Management and Resilience		
Incident Resilience Planning and Strategy/Testing: Scenarios are used to improve incident detection and response.	Source: IS.II.C.21:pg43: Management should test information security incident scenarios.	Arctic Wolf facilitates incident response plans through its Incident Response Simulation Service that runs through live table-top exercises, makes recommendations, and addresses regulatory requirements.
Detection, Response & Mitigation/ Detection: Alert parameters are set for detecting information security incidents that prompt mitigating actions.	Source: IS.II.C.15(a):pg32: To prevent unauthorized access to or inappropriate activity on the operating system and system utilities, filter and review logs for potential security events and provide adequate reports and alerts. IS.II.C.15(b):pg33: Management should implement effective application access controls by logging access and events, defining alerts for significant events, and developing processes to monitor and respond to anomalies and alerts.	Arctic Wolf's managed detection and response service provides unlimited flexibility in tailoring services to a financial institution's specific monitoring needs. The Arctic Wolf Customized Rule Engine (CRulE) allows the Arctic Wolf CST to apply precise security policies, updating them as needed to align with changing business needs. The AWN CyberSOC ingests, parses and analyses network and log data and provides both automated and custom reports.
Detection, Response & Mitigation/ Detection: Tools and processes are in place to detect, alert, and trigger the incident response program.	Source: IS.III.D:pg50: The institution's program should have defined protocols to declare and respond to an identified incident.	The AWN CyberSOC provides an outcome-based service that detects, alerts and responds to advanced attacks that may bypass existing perimeter controls. The Arctic Wolf Concierge Security™ team (CST) provided by the AWN CyberSOC service functions as a single point of contact that can tailor the Arctic Wolf managed detection and response (MDR) service to fit a financial institution's needs.
Detection, Response & Mitigation/ Response and Mitigation: Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information.	Source: IS.III.D:pg52: While containment strategies between institutions can vary, they typically include isolation of compromised systems or enhanced monitoring of intruder activities, search for additional compromised systems, collection and preservation of evidence.	The Arctic Wolf CST prioritizes incidents and identifies critical remediation steps that a financial institution IT team should take. The Arctic Wolf CST proactively hunts for hidden threats, performs remote forensics analysis of incidents and provides actionable plans to help remediate incidents.

FFIEC/NCUA Control Objective	FFIEC/NCUA Control Activity (abbreviated)	AWN CyberSOC™ Service Capability
Escalation and Reporting/ Escalation and Reporting: A process exists to contact personnel who are responsible for analyzing and responding to an incident.	Source: IS.III.C:pg50: Escalation policies should address when different personnel within the organization will be contacted and the responsibility those personnel have in incident analysis and response.	The Arctic Wolf CST prioritizes incidents and identifies remediation steps needed to respond to an incident. Institutions have direct access to the Arctic Wolf CST by phone or email. Every customer is assigned their own Arctic Wolf CST that is backed by a team of experts across every key security domain.
Escalation and Reporting/ Escalation and Reporting: Incidents are classified, logged, and tracked.	Source: OPS.B.28: Event/problem management plans should cover hardware, operating systems, applications, and security devices and should address at a minimum: event/ problem identification, etc.	AWN CyberSOC tracks incidents in the customer portal, as well as through monthly check-ins with the Arctic Wolf CST, and executive summary reports.

References

- FFIEC Cybersecurity Assessment Tool Appendix A: Mapping Baseline Statements to FFIEC IT Examination Handbook (June 2015) - https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_A_Map_to_FFIEC_Handbook_June_2015_PDF3.pdf
- FFIEC Information Technology Examination Handbook: Information Security (September 2016) - FFIEC Information Technology Examination Handbook: Information Security Booklet - https://www.ffiec.gov/press/pdf/ffiec_it_handbook_information_security_booklet.pdf
- FFIEC Information Technology Examination Handbook: Operations (July 2004) - https://ithandbook.ffiec.gov/media/274825/ffiec_itbooklet_operations.pdf

About Arctic Wolf

Arctic Wolf Networks provides SOC-as-a-service that redefines the economics of security. The AWN CyberSOC™ service is anchored by Concierge Security™ teams and includes 24×7 monitoring, custom alerting and incident investigation and response. There is no hardware or software to purchase, and the end-to-end service includes a proprietary cloud-based SIEM, threat intelligence subscriptions and all the expertise and tools required. For more information about AWN CyberSOC, visit https://arcticwolf.com.