ARCTIC WOLF

BRIEF

A Cybersecurity Risk Checklist for Financial Institutions

For organizations in financial services, compliance concerns come from a variety of laws, guidelines, and industry rules, including:

- The Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Bank Secrecy Act (BSA)
- New York State Department of Financial Services 23 NYCRR 500 (for firms in New York state)
- Federal Financial Institutions Examination Council/ National Credit Union Administration (FFIEC/NCUA) Guidelines

Small and midsize financial institutions such as regional banks and credit unions operate under a microscope of regulatory scrutiny. Deviating from federal and state rules and guidelines can ultimately result in lengthy periods placating regulators, as well as an escalating risk of penalties and liabilities. In addition to compliance, financial institutions need to be concerned with fraud, cyberattacks, and reputational harm.

Addressing Cybersecurity-Specific Rules

Navigating the many cybersecurity-specific requirements is one of the biggest challenges in complying with financial regulations and guidelines. These include:

- Identifying internal and external vulnerabilities
- 24x7 security monitoring
- Log aggregation and management
- Tracking user access and login attempts
- Developing a thorough incident response plan

Small and midsize financial institutions face some significant hurdles in meeting compliance obligations. The pressure is further compounded since financial institutions are among the most heavily targeted organizations by cybercriminals.

For financial institutions like regional banks and credit unions, building an in-house security operations center (SOC) for comprehensive cybersecurity often isn't realistic, as the cost of recruiting and retaining in-house security talent can be prohibitive with security experts in high demand amid a growing skills shortage. But investing in more point solutions is not the answer. Even the best firewalls and intrusion detection systems are not designed to holistically manage cyber risk or provide a flexible framework for real-time, incident response. What financial institutions need are security systems, processes, and personnel on par with large enterprises. But how can they attain that?

The Arctic Wolf SOC-as-a-service helps financial institutions manage cyber risk while, at the same time, also meet compliance requirements. It starts with an expert team of security analysts and incident responders who continuously monitor your network for potential cyberthreats and respond to incidents as they arise. The service includes centralized logging of all network events, vulnerability assessments to identify risks, and a detailed framework for managing compliance in accordance with security regulations and guidelines.

The following checklist identifies key facets of comprehensive cybersecurity that Arctic Wolf addresses for financial institutions.

Cybersecurity Requirement	The Arctic Wolf SOC-as-a- Service
Compliance:	
Compliance management and reporting: Assess a financial institution's security to identify and report on instances of non-compliance with federal, state, and local regulations and guidelines	
Workflow integration: Seamless integration with existing IT workflows ensures that financial firms' personnel are notified of non-compliance issues and security escalations in a timely manner	
Risk Assessment:	
Vulnerability scanning: Regularly scheduled vulnerability assessments provide actionable recommendations to strengthen overall security posture and address potential sources of cyber risk as they arise	
Monitoring, Detection, and Response:	
Log data collection and correlation: Log data aggregation centralizes up to billions of daily events generated through security solutions, network devices, endpoints, and applications into a single console for real-time threat monitoring	
Continuous network monitoring: Dedicated security analysts analyze log data 24/7 using advanced processes such as machine intelligence to filter through thousands of network alerts into a few incidents that warrant manual investigation	
Cloud and on-premises monitoring: Continuous network monitoring applies to the entirety of a financial firm's IT ecosystem, including all on-premises resources as well as all cloud-based services that comprise a hybrid IT environment	
Incident Response:	
A named security team: A dedicated team of security experts that work directly with the financial firms they serve, giving each organization a complete picture of its unique operational circumstances	
Incident response processes: Incident responders act the moment a threat is detected to quarantine, contain, and remediate the incident	

Protect Your Financial Institution with Arctic Wolf's Subscription Service

Arctic Wolf provides financial institutions, including regional banks and credit unions, with the services they need to operate in compliance and stay safe from cyberthreats and accidental data breaches. The company offers predictable pricing through a subscription service based on the number of users, servers, and locations—not the number of events or log volumes. With around-the-clock access to a Concierge Security™ Team (CST), continuous threat detection and response, regular vulnerability scans, and cybersecurity-specific compliance management, Arctic Wolf helps ensure that the sensitive data of financial institutions remains secure.

ARCTIC WOLF

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com