ALERT LOGIC™

SOLUTION BRIEF

Alert Logic™ Solutions for FFIEC/GLBA Compliance

Introduction

The Federal Financial Institutions Examination Council (FFIEC) makes recommendations to promote uniformity in the supervision of financial institutions. Financial institutions must comply with the guidelines of FFIEC as issued pursuant to the Gramm-Leach-Bliley Act of 1999 (GLBA).

The governing bodies and affected entities in scope for FFIEC compliance are:

GOVERNING BODY	AFFECTED ENTITY
Board of Governors of the Federal Reserve System (FRB)	• State member • Bank holding • Nonbank subsidiaries of bank holding • Savings and loan holding • Edge and agreement • Branches and agencies of foreign banking organizations operating in the United States and their parent banks • Officers, directors, employees, and certain other categories of individuals associated with the above banks, companies, and organizations (referred to as “institution-affiliated parties”)
Federal Deposit Insurance Corporation (FDIC)	• Insured state chartered banks that are not members of the Federal Reserve System (state nonmember banks) • Insured FOREIGN branches • Officers, directors, employees, controlling shareholders, agents, and certain other categories of individuals (institution-affiliated parties) associated with such institutions

GOVERNING BODY	AFFECTED ENTITY
National Credit Union Administration (NCUA)	• Credit unions
Office of the Comptroller of the Currency (OCC)	• National banks and their subsidiaries • Federally chartered savings associations and their subsidiaries • Federal branches and agencies of foreign banks • Institution-affiliated parties (IAPs), including (a) officers, directors, and employees, and (b) a bank's controlling stockholders, agents, and certain other individuals

Alert Logic solutions can help companies with their FFIEC/GLBA compliance projects with less complexity, and at a fraction of the total cost and time of traditional security tools. Alert Logic integrates cloud-based software, analytics and expert services to assess, detect and block threats to applications and environments to improve your security visibility. We focus on the threats most relevant to cloud-hosted applications by defending each layer of your application and infrastructure stack against hard-to-detect web application attacks. Integrated expert services augment your in-house security team by monitoring your cloud workloads and environment 24/7.

Analysts investigate alerts and contact you within 15 minutes if we detect suspicious activity such as: unauthorized access, exposure or modification of accounts, controls or configurations.

Requirements and Solutions

FFIEC's security recommendations are based on NIST SP800-33:

- **Availability –** The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.
- **Integrity of Data or Systems –** System and data integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
- **Confidentiality of Data or Systems –** Confidentiality covers the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use.
- **Accountability –** Clear accountability involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.
- **Assurance –** Assurance addresses the processes, policies, and controls used to develop confidence that technical and operational security measures work as intended. Assurance levels are part of the system design and include availability, integrity, confidentiality, and accountability. Assurance highlights the notion that secure systems provide the intended functionality while preventing undesired actions.

FFIEC REQUIREMENT	SUMMARY	ALERT LOGIC SOLUTION
Security Process	Financial institutions should implement an ongoing security process and institute appropriate governance for the security function, assigning clear and appropriate roles and responsibilities to the board of directors, management, and employees (institution-affiliated parties) associated with such institutions.	Alert Logic helps organizations to better understand their risks of data loss and breaches and recommends appropriate services or products to fill those voids. Alert Logic is a supporting tool for security management decision making. Auditors can validate presence and review of controls with Alert Logic Professional
Information Security Risk Assessment	Financial institutions must maintain an ongoing information security risk assessment program that effectively: • Gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements • Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets • Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation	Alert Logic's primary value is to provide direct support to monitoring the Electronic Security Perimeter and Critical Cyber Assets. Also supports identification of configuration changes for perimeter devices. Cyber Vulnerability Assessments (CVA) are enhanced by Alert Logic's ability to collect detected vulnerabilities during ongoing operations, providing protection beyond the "point-in-time" nature of a CVA.
Information Security Strategy	Financial institutions should develop a strategy that defines control objectives and establishes an implementation plan. The security strategy should include: • Appropriate consideration of prevention, detection, and response mechanisms • Implementation of the least permissions and least privileges concepts • Layered controls that establish multiple control points between threats and organization assets • Policies that guide officers and employees in implementing the security program	Alert Logic is a supporting tool for security management decision making. Auditors can validate presence and review of controls with Alert Logic Professional. Alert Logic enhances staff training by providing an additional mechanism to monitor company activities. Alert Logic's ActiveWatch service provides human 24/7 monitoring by trained information security professionals, and live access to certified security professionals for on-demand consultation

FFIEC REQUIREMENT	SUMMARY	ALERT LOGIC SOLUTION
Security Controls Implementation	The goal of access control is to allow access by authorized individuals and devices and to disallow access to all others. An effective control mechanism includes numerous controls to safeguard and limits access to key information system assets at all layers in the network stack. This section addresses logical and administrative controls, including access rights administration for individuals and network access issues. A subsequent section addresses physical security controls. • Access Rights Administration • Authentication • Network Access • Operating System Access • Application Access • Remote Access	Alert Logic provides a centralized system for collecting, reporting, and alarming on security compliance events.
Security Monitoring	Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by: • Monitoring network and host activity to identify policy violations and anomalous behavior • Monitoring host and network condition to identify unauthorized configuration and other conditions which increase the risk of intrusion or other security events • Analyzing the results of monitoring to accurately and quickly identify, classify, escalate, report, and guide responses to security events • Responding to intrusions and other security events and weaknesses to appropriately mitigate the risk to the institution and its customers, and to restore the institution's systems	Alert Logic's primary value is to provide direct support to monitoring the Electronic Security Perimeter and Critical Cyber Assets. Also supports identification of configuration changes for perimeter devices. Cyber Vulnerability Assessments (CVA) are enhanced by Alert Logic's ability to collect detected vulnerabilities during ongoing operations, providing protection beyond the "point-in-time" nature of a CVA.
Security Process Monitoring and Updating	Financial institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. They should then use that information to update the risk assessment, strategy, and implemented controls.	Alert Logic Professional provides the ability for scanning internal and external hosts for known vulnerabilities/missing patches and detects security incidents. It also includes a knowledge base for remediation steps. It detects and alerts to security events and incidents as they happen.