

# ALERT LOGIC® SOLUTIONS FOR FFIEC/GLBA COMPLIANCE

## INTRODUCTION

The Federal Financial Institutions Examination Council (FFIEC) is a formal inter-agency body of the United States government empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by 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 (CFPB). 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)	<ul style="list-style-type: none"><li>• STATE MEMBER</li><li>• BANK HOLDING</li><li>• NONBANK SUBSIDIARIES OF BANK HOLDING</li><li>• SAVINGS AND LOAN HOLDING</li><li>• EDGE AND AGREEMENT</li><li>• BRANCHES AND AGENCIES OF FOREIGN BANKING ORGANIZATIONS OPERATING IN THE UNITED STATES AND THEIR PARENT BANKS</li><li>• OFFICERS, DIRECTORS, EMPLOYEES, AND CERTAIN OTHER CATEGORIES OF INDIVIDUALS ASSOCIATED WITH THE ABOVE BANKS, COMPANIES, AND ORGANIZATIONS (REFERRED TO AS “INSTITUTION-AFFILIATED PARTIES”)</li></ul>

GOVERNING BODY	AFFECTED ENTITY
FEDERAL DEPOSIT INSURANCE CORPORATION (FDIC)	<ul style="list-style-type: none"> <li>INSURED STATE CHARTERED BANKS THAT ARE NOT MEMBERS OF THE FEDERAL RESERVE SYSTEM (STATE NONMEMBER BANKS)</li> <li>INSURED FOREIGN BRANCHES</li> <li>OFFICERS, DIRECTORS, EMPLOYEES, CONTROLLING SHAREHOLDERS, AGENTS, AND CERTAIN OTHER CATEGORIES OF INDIVIDUALS (INSTITUTION-AFFILIATED PARTIES) ASSOCIATED WITH SUCH INSTITUTIONS</li> </ul>
NATIONAL CREDIT UNION ADMINISTRATION (NCUA)	<ul style="list-style-type: none"> <li>CREDIT UNIONS</li> </ul>
OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC)	<ul style="list-style-type: none"> <li>NATIONAL BANKS AND THEIR SUBSIDIARIES</li> <li>FEDERALLY CHARTERED SAVINGS ASSOCIATIONS AND THEIR SUBSIDIARIES</li> <li>FEDERAL BRANCHES AND AGENCIES OF FOREIGN BANKS</li> <li>INSTITUTION-AFFILIATED PARTIES (IAPS), INCLUDING (A) OFFICERS, DIRECTORS, AND EMPLOYEES, AND (B) A BANK'S CONTROLLING STOCKHOLDERS, AGENTS, AND CERTAIN OTHER INDIVIDUALS</li> </ul>

With limited resources and increasing use of cloud and virtualization, compliance has become more challenging. Alert Logic plays a vital role in an agency's FFIEC/GLBA compliance efforts by providing fully managed Security-as-a-Service solutions that can be deployed in on-premises data centers, hosted environments, or in public and private clouds, providing a single view and unified reporting on an agency's entire infrastructure. Alert Logic's security portfolio addresses the most relevant infrastructure threats with intrusion detection, vulnerability scanning, log management and storage, web application security, and a 24x7 Security Operations Center staffed by GIAC-certified experts to provide monitoring and response guidance.

## 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
<b>SECURITY PROCESS</b>	<p>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.</p>	<p>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 within Alert Logic® Threat Manager™, Alert Logic® Log Manager™ and Alert Logic® Web Security Manager™</p>
<b>INFORMATION SECURITY RISK ASSESSMENT</b>	<p>Financial institutions must maintain an ongoing information security risk assessment program that effectively:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• Analyzes the probability and impact associated with the known threats and vulnerabilities to their assets</li> <li>• Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation</li> </ul>	<p>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.</p>
<b>INFORMATION SECURITY STRATEGY</b>	<p>Financial institutions should develop a strategy that defines control objectives and establishes an implementation plan. The security strategy should include:</p> <ul style="list-style-type: none"> <li>• Appropriate consideration of prevention, detection, and response mechanisms</li> <li>• Implementation of the least permissions and least privileges concepts</li> <li>• Layered controls that establish multiple control points between threats and organization assets</li> <li>• Policies that guide officers and employees in implementing the security program</li> </ul>	<p>Alert Logic is a supporting tool for security management decision making. Auditors can validate presence and review of controls within Threat Manager, Log Manager and Web Security Manager.</p> <p>Alert Logic enhances staff training by providing an additional mechanism to monitor company activities. Alert Logic's ActiveWatch service provides human 24x7 monitoring by trained information security professionals, and live access to certified security professionals for on-demand consultation</p>

FFIEC REQUIREMENT	SUMMARY	ALERT LOGIC SOLUTION
<p><b>SECURITY CONTROLS IMPLEMENTATION</b></p>	<p>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.</p> <ul style="list-style-type: none"> <li>• Access Rights Administration</li> <li>• Authentication</li> <li>• Network Access</li> <li>• Operating System Access</li> <li>• Application Access</li> <li>• Remote Access</li> </ul>	<p>Alert Logic provides a centralized system for collecting, reporting, and alarming on security compliance events.</p> <p>Alert Logic Log Manager and Threat Manager, and Web Security Manager are rapid deployment Software-as-a-Service solutions that quickly address the technology requirements.</p>
<p><b>SECURITY MONITORING</b></p>	<p>Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by:</p> <ul style="list-style-type: none"> <li>• Monitoring network and host activity to identify policy violations and anomalous behavior</li> <li>• Monitoring host and network condition to identify unauthorized configuration and other conditions which increase the risk of intrusion or other security events</li> <li>• Analyzing the results of monitoring to accurately and quickly identify, classify, escalate, report, and guide responses to security events</li> <li>• 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</li> </ul>	<p>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.</p>
<p><b>SECURITY PROCESS MONITORING AND UPDATING</b></p>	<p>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.</p>	<p>Threat Manager 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.</p>