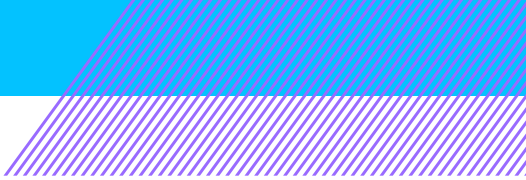**ULTIMATE GUIDE TO**

Monitoring and Logging Requirements for Compliance

With new data breaches announced almost daily, legislative bodies no longer trust organizations to protect their data. Most recently, in the United States, the **New York Department of Financial Services (NY DFS) brought charges** against a company that knew about its control weaknesses from "at least October 2014 through May 2019" and ignored its internal experts, choosing to do nothing to remediate the situation. Ultimately, this left more than 850 records containing non-public personal information (NPI) exposed to the public.

graylog

TABLE OF CONTENTS

With new data breaches announced almost daily, legislative bodies no longer trust organizations to protect their data. Most recently, in the United States, the **New York Department of Financial Services (NY DFS) brought charges** against a company that knew about its control weaknesses from "at least October 2014 through May 2019" and ignored its internal experts, choosing to do nothing to remediate the situation. Ultimately, this left more than 850 records containing non-public personal information (NPI) exposed to the public.

While not all organizations ignore cybersecurity so egregiously, stories like these give governmental bodies reason to distrust corporate cybersecurity. As recently as October 2020, the NY DFS took another bold step suggesting that since social media platforms influence financial markets, they should be subject to regulatory requirements governing cybersecurity, similar to financial services institutions.

Although no one has a crystal ball, most security professionals agree that newer and more stringent regulations will continue to be enacted over the next five to ten years. With that in mind, taking a look at the current laws and industry standards provide insight into the types of controls organizations need. Nearly every law and standard lists event logs as a primary requirement because they report some of the most detailed information about an organization's IT ecosystem.
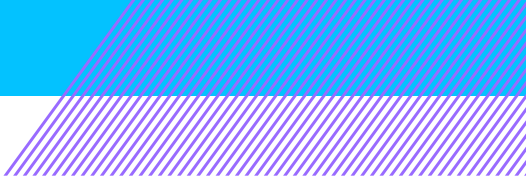
Every technology, from Software-as-a-Service application to on-premises server, generates event log data around a variety of different activities. This data provides details about actions taken within the ecosystem, giving valuable insight that enables preventative threat monitoring and detective forensic evidence. When compliance standards require "continuous monitoring" as a proactive risk mitigation control, they often mean looking at event log data to detect anomalies that indicate potential cybercriminal interference. What compliance requirements often ignore, however, is the need to standardize the data appropriately to obtain enough details for meaningful threat detection without collecting so much information that security teams become overwhelmed.

Top 5 Most Important Cybersecurity and Privacy Regulations

Detailing every cybersecurity or privacy regulation requiring continuous monitoring would not only take months, but it would also become repetitive. Most standards and regulations mimic one another, although some landmark laws and industry standards exist. For example, the NY DFS Cybersecurity Regulation may only apply to financial services companies incorporated or doing business in New York state. However, that regulation was also the first one to include continuous monitoring requirements and enhanced liability for data breaches arising from third-party vendors. With that in mind, the following list of regulations and standards is not exhaustive but provides examples that showcase both the commonalities between and evolution of cybersecurity and privacy compliance.

① The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Although targeted at healthcare organizations and their business associates, HIPAA was one of the first broad-reaching security and privacy laws in the United States. The regulation consists of four rules: Security Rule, Privacy Rule, Breach Notification Rule, and Enforcement Rule. In 2013, the Department of Health and Human Services (HHS), the agency that enforces HIPAA, announced the Omnibus Rule, which implemented multiple provisions in the Health Information Technology for Economic and Clinical Health Act (HITECH) as part of HIPAA compliance. The **Omnibus Rule** applied four penalty tiers based on violation categories that ranged from "unknowing" violations with a minimum of $100 per violation to "willful neglect" with a minimum of $50,000 per violation.

The **Security Rule** breaks down into three categories of safeguards: administrative, physical, and technical. Within these safeguards, controls can be deemed "required" or "addressable." Organizations must implement Required safeguards as written in the law. Meanwhile, Addressable safeguards, while not optional, can be implemented in ways that prove less burdensome than as defined in the law.

Under the Administrative Safeguards, HIPAA defines several Required controls that relate to log management:

- **Information system activity review (Required).** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports

- **Response and Reporting (Required).** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Under the Technical Safeguards, HIPAA's Security Rule requires:

- **Standard: Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronically protected health information.

Additionally, some Addressable controls that relate to log management include:

- **Log-in monitoring (Addressable).** Procedures for monitoring log-in attempts and reporting discrepancies.

- **Integrity controls (Addressable).** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

HIPAA's Required and Addressable controls can be viewed as fundamental event log data across the security and privacy regulatory landscape.

② Gramm-Leach-Bliley Act (GLBA)

GLBA, also referred to as the Financial Services Modernization Act of 1999, protects consumer financial privacy. Enforced by the Federal Trade Commission (FTC) and various other federal agencies, GLBA consists of the Financial Privacy Rule, Safeguards Rule, and Pretexting provisions. While the Financial Privacy Rule focuses on data collection and disclosure, the Safeguards Rule sets forth the requirements for securing data.

As another early privacy legislation, GLBA does not directly mention event logs. Despite this, the following provision can be deemed an early data privacy and security clause:

> (b) FINANCIAL INSTITUTIONS SAFEGUARDS.—In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—
>
> (1) to ensure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use such records or information, resulting in substantial harm or inconvenience to any customer.

By modern standards, the Safeguards Rule is vague and outdated. In 2019, however, the **FTC solicited public comments on proposed rule changes.** These changes seek to update the law to align better with digital transformation cybersecurity concerns. The proposed changes look to clarify best practices, including more detailed requirements such as:

- Continuous monitoring for real-time threat intelligence

- Establishment of audit trails to detect compromises or attempted compromises to information systems

- Change management procedures

- User access monitoring to detect authorized user activities or unauthorized data access, use, or changes

Although these updates to GLBA have not yet been finalized, they indicate that the FTC seeks to align GLBA with other cybersecurity and privacy requirements. Thus, event logs that provide visibility into anomalous activities signaling potential data security events will apply more specifically to GLBA in the future.

③ Sarbanes-Oxley Act of 2002 (SOX)

SOX directly responded to the Enron, Tyco International, and WorldCom corporate financial scandals in the early 2000s. Enacted in 2002, SOX set forth strict rules for financial reporting, looking to increase investor confidence.

Although organizations engaged in some digital transactions in 2002, the accelerated pace of digital transformation through the 2000s and 2010s transitioned Section 404 "Management assessment of internal controls" into an IT compliance mandate. Section 404 states:

EC. 404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.

(a) RULES REQUIRED.—The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

(b) INTERNAL CONTROL EVALUATION AND REPORTING.—With Respect to the internal control assessment required by subsection(a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.
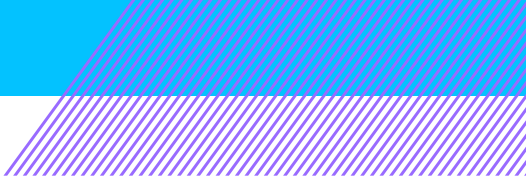
SOX set forth the requirement that organizations prevent insider fraud by establishing Segregation of Duties (SoD), ensuring no conflict of interest exists. For example, the same person who creates new vendor accounts in a company's payment system should not also be allowed to pay vendors. The goal is to remove any conflicts of interest that could enable users to engage in insider fraud.

As organizations moved to Cloud-First or Cloud-Only models, Identity and Access Governance became a fundamental SOX control. Event logs that fall under the SOX umbrella include:

- User Login
- User Logoff
- Logon Failure
- Audit Logs Access
- Object Access
- System Events
- Host Session Status
- Security Log Archiving

- Track Account Management Changes
- Track User Group Changes
- Track Audit Policy Changes
- Successful User Account Validation
- Unsuccessful User Account Validation
- Track Individual User Actions
- Track Application Access

④ Payment Card Industry Data Security Standard (PCI DSS)

While HIPAA, GLBA, and SOX are regulations with the force of law, PCI DSS is an industry-standard that established prescriptive controls for any organizations that collect payment. Although many see this as a compliance standard focused on retail, any organization that accepts credit card payments needs to meet the standard, including healthcare, entertainment, and financial institutions.

In the early 2000s, the Payment Card Industry Security Standards Council was founded by the five major payment card companies, American Express, Discover Financial Services, JCB International, MasterCard, and Visa, Inc. As part of the initiative to protect cardholders from credit card fraud, they established PCI DSS in 2004. The standard applies penalties to non-compliant merchants ranging from $5,000 to $100,000 per month, depending on the violation's severity.

Consisting of twelve requirements, PCI DSS sets forth clearly defined controls. Organizations that collect credit card data need to protect the sensitive authentication data (SAD) and cardholder data (CHD), which is defined as the Primary Account Number (PAN) or the PAN and cardholder name, card expiration date, service code, or Sensitive Authentication Data such as full magnetic stripe data, CAV2, CVC2, CVVV2, CID, PINs and PIN blocks.

"Requirement 10: Track and monitor all access to network resources and cardholder data" details the audit logs necessary to prove compliance, including:

- Access to cardholder data

- Actions taken by individuals with root or administrative privileges

- Access to audit trails

- Invalid logical access attempts

- Identification and authentication mechanisms

- Privilege elevation

- Changes, additions, or deletions to accounts with root or administrative privileges

- Initialization of audit logs

- Stopping or pausing audit logs

- Creation and deletion of system-level objects

- External facing technologies such as wireless, firewalls, DNS, and mail

- All security events

- System components that store, process, or transmit CHD and/or SAD

- Critical system components

- Servers and system components that perform security functions, such as firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, and e-commerce redirection servers

Information that should be collected for each of these types of logs includes:

- User ID

- Event type

- Date and time

- Success or failure

- Origin of event

- Identity or name of affected data, system component, or resource

To meet PCI DSS compliance, organizations subject to the standard must engage in and document periodic reviews. Unlike many other regulations and standards, PCI DSS provides clear, step-by-step lists of the event log documentation necessary to meet compliance.

⑤ European Union General Data Protection Regulation (GDPR)

Enacted in 2016 and implemented in 2018, the **GDPR** is a landmark data privacy regulation. It stands as the first regulation providing for extra-territorial jurisdiction, applying to organizations outside the European Union (EU) to the extent that they collect, transmit, or store non-public personal information (NPI) for EU citizens or non-EU citizens living in the EU. Under the GDPR, non-compliance can lead to fines up to €10 million or 2% of an organization's total worldwide annual turnover of the preceding financial year.

Chapter 4, Article 25, sets forth the concept of "Data protection by design and default," requiring companies to:

- Implement appropriate technical and organizational measures, such as pseudominisation, which are designed to implement data protection principles such as data minimization.

- Implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

Going into further detail, Chapter 4, Article 32, "Security of processing" requires that companies:

- Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

- Assessing the appropriate level of security necessary to protect data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

Finally, the GDPR requires organizations to notify their supervisory authorities of a data breach no later than 72 hours after identifying the event. The notification needs to include:

- The data categories

- Approximate number of data subjects impacted

- Approximate number of personal data records concerned

- Describe the likely consequences of the personal data breach

- Describe the measures taken or proposed to be taken to address the breach

- Measures to mitigate possible adverse effects

While the GDPR, as with other non-prescriptive compliance requirements, does not list specific event logs, the information they contain helps proactively detect potential security events and provides investigative data that helps meet the breach reporting requirement.

Generalized Requirements

Despite the depth and breadth of regulatory and industry-standard compliance requirements, most map to one or more cybersecurity frameworks. While the cybersecurity frameworks may contain different vocabulary, they all generally require similar controls and documentation to assure compliance.

Set the right controls

Many organizations need to comply with multiple regulations and industry standards. For example, a healthcare provider needs to meet HIPAA and PCI DSS compliance, while a publicly traded global enterprise needs to meet SOX and GDPR requirements.

Fundamentally, however, all regulations and industry standards rely on one or more cybersecurity frameworks when choosing the right controls. For example, HIPAA maps to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and the International Organization for Standardization (ISO) 27001:2013. Meanwhile, PCI DSS maps to both NIST 800-53 and the **Center for Internet Security (CIS) Controls**.

Although NIST SP 800-53, ISO 27001:2013, and CIS Controls incorporate many of the same controls, they also use their own terminology, creating a challenge for many organizations. Bringing all three together, as evidenced in Appendix A, the different controls align with the following categories:

- Identity and Access Management
- Configuration Management
- Information Security Program Adoption
- Continuous Vulnerability Monitoring
- Incident Detection and Response

When planning a log collection and management strategy, an organization should first set controls that align with these five primary control groups.

Collect the right stuff

Collecting too much data leaves the organization's security team overwhelmed while collecting too little information leaves the compliance team unable to provide the appropriate documentation for proving governance.

Once the organization establishes security controls based on its risk tolerance level, it needs to collect data that can alert the security team to potential threats and document its adherence to policies for the auditor.

Determining the most critical event logs to collect can be overwhelming, especially when the organization needs to meet multiple compliance requirements across more than one cybersecurity framework. Appendix B details the event logs suggested by CIS, NIST 800-53, and ISO 27001:2013. From a high level, organizations should collect, at minimum collect
data across the following six categories:

- **Audit and Accountability:**
  - User activity
  - Network connected systems and devices
  - Event source, date, user, timestamp, source address

- **Identity and Access Management:**
  - Device authentication and authorization
  - User access to resources
  - Failed login attempts
  - Privileged access use
  - Remote logins
  - Application access

- **Configuration and Change Management:**
  - Unauthorized changes
  - Enforcement of access restrictions

- **Continuous Controls Monitoring:**

  – System and application vulnerabilities
  – Comparison of vulnerability scans
  – Unauthorized traffic
  – Risk-based prioritization of vulnerabilities

- **System Communications and Protection:**

  – Unauthorized inbound network traffic, including systems, users, and applications
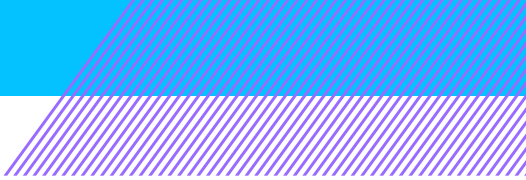 – Unauthorized outbound network traffic, including systems, users, and applications

- **Incident Detection and Response:**

  – Unauthorized commands
  – Intrusion Detection Systems/Intrusion Prevention Systems data
  – Incident scoring schema

Continuously Monitor and Document THE Controls' Effectiveness

Nearly every regulation and industry standard requires continuous controls monitoring. However, some organizations struggle as they still adhere to analog point-in-time audit mentalities. Since malicious actors continuously evolve their threat methodologies, organizations need to monitor their controls' effectiveness continuously and document their processes as part of their proactive threat hunting process.

To protect against cyberattacks, organizations need to not only collect event log data but review it. As part of continuous monitoring, organizations should regularly review logs to detect anomalies indicating a potential cyber attack. For example, unsuccessful login reports can indicate a password spray or attempted credential theft. Meanwhile, unauthorized software installation might mean malware executing on a device.

NIST SP 800-53 notes explicitly, "RA-10: Establish and maintain a cyber threat hunting capability to search for indicators of a compromise and detect, track, and disrupt threats that evade existing controls."

Continuously monitoring controls, documenting anomalies, and remediating detected weaknesses creates a "security-first" approach to compliance. Cybersecurity professionals recognize that compliance is not equal to security, so they should focus on documenting their security work for better audit outcomes. When security is the primary focus, compliance often follows nearly effortlessly.
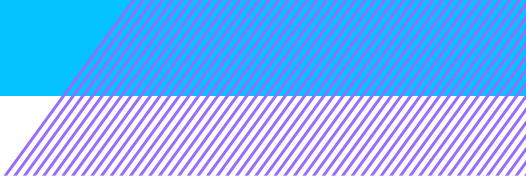
Insider Threat

Three categories of insider threats impact organizations:

1. Some employees look to steal from organizations.

2. Workforce members often have too much access within an organization's IT stack, creating a risk of accidental privilege misuse.

3. Cybercriminals often steal user credentials so that they can move around within a company's ecosystem undetected.

Log data provides visibility into all three of these risks. Monitoring user access, especially privileged access, enables organizations to protect the Identity perimeter. Some log event data that can help detect insider threats or credential theft include:

- Anomalous access to sensitive data unrelated to user job function may indicate accidental privilege misuse.

- Activity outside of regular user work hours may indicate a malicious insider looking to steal data.

- Activity from the wrong IP address may indicate credential theft.

Consolidating all log information in a single location gives security teams more visibility into potential anomalous activities, potentially indicating an insider threat. Purposefully choosing the correct user access event log data and establishing a risk-based alert prioritization process reduces alert fatigue and enables rapid response to these types of data security events.

Retain logs

Although some regulations require log retention for a specified time period, many organizations also keep event data for audit documentation and reactive forensic analysis. Since malicious actors that infiltrate systems and networks can dwell for days, months, or years, organizations need to ensure that they have all the evidence necessary for security event research.

Only CIS specifically references event log retention:

- **6.6: Deploy SIEM or log analytic tools:** Deploy Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis.

- **6.4: Ensure adequate storage for logs:** Ensure that all systems that store logs have adequate storage space for the logs generated.

Prove you are following your policies

Auditors need documentation that proves the organization is following its policies. Although cybersecurity professionals may like to lay claim to the "trust but verify" mantra, auditors have been following that since before the internet.

Event log data enables more robust compliance by providing objective documentation that proves the organization follows its internal controls. For example, user activity and access exception data prove that the enterprise enforces the principle of least privilege or makes purposeful decisions when making emergency access exceptions.

Prevent logs from being tampered with

Although protecting log data against tampering appears to be common sense, human error can often find its way into any manual process.

ISO 27001:2013 is the only cybersecurity framework to address log tampering, noting specifically:

- **A.12.4.2:** Logging facilities and log information shall be protected against tampering and unauthorized access.

- **A.18.1.3 Protection of records:** Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, contractual, and business requirements.

Since event logs can highlight external and internal malicious activity, organizations need to place security controls around who accesses them and where they are stored. At a minimum, organizations need to limit log data access. Some suggestions for controls include:

- Incorporating event log data access into organizational access policies

- Applying the principle of least privilege to log data

- Defining categories of users who can edit or view data

- Applying privileged access controls around event log data edit entitlements

Use in Forensics

No matter how hard an organization works to protect itself from a cyberattack, it will likely experience a data security event. Most cybersecurity professionals agree that the days of "if an attack" are gone, and they now look to managing the "when an attack" occurs.

Event log data, if properly collected, can provide visibility into how an attacker infiltrated an organization's systems, networks, devices, and software. For example, configuring network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to a wired network can provide insight into when or how a cybercriminal remotely accessed the enterprise infrastructure.

Breach Response Process

Organizations need to prove security controls' effectiveness and meet strict breach notification rules. For example, the GDPR established a 72-hour breach notification rule that requires organizations to include information like the nature of the breach, information categories stolen, the approximate number of data subjects impacted likely consequences, and remediation steps taken.

When organizations efficiently collect event log data, they can more rapidly determine the source of the data breach and reduce mean time to resolution. By carefully choosing how to aggregate and correlate log data, organizations can use automation more effectively, ultimately reducing the number of false positives, alert fatigue, and time taken to research the breach.

Additionally, log event collection and correlation enables organizations to document their breach response process and prove they complied with regulatory breach notification requirements.
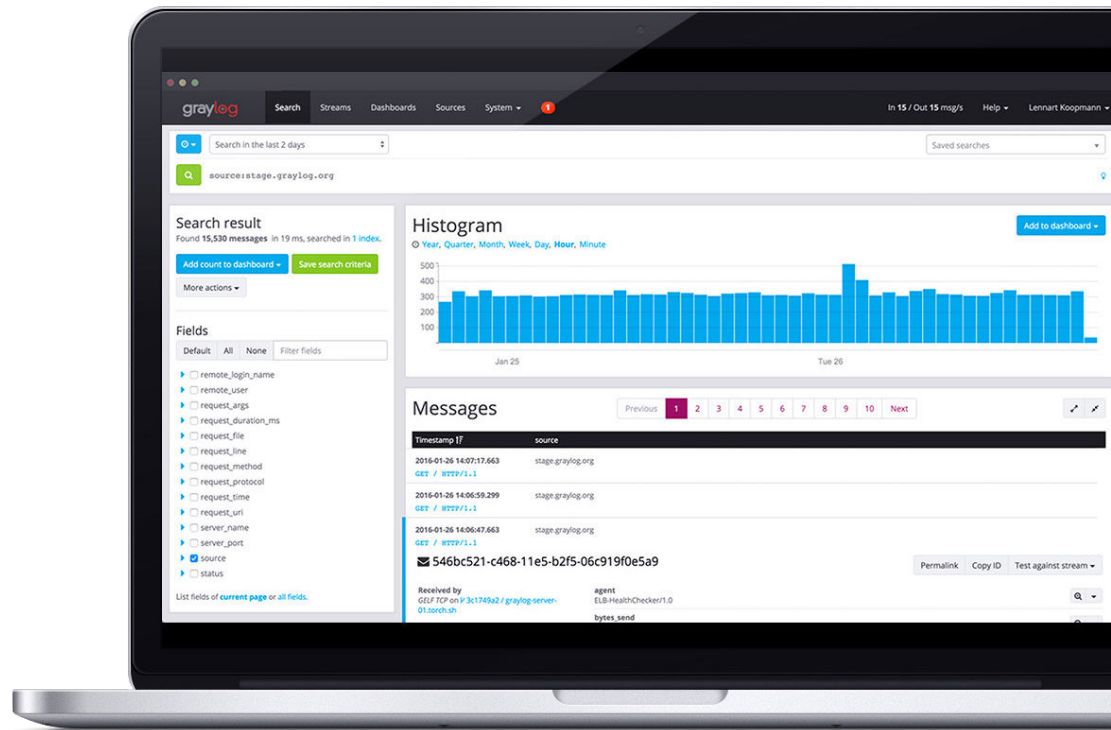
About Graylog

Graylog is a leader in log management and Security Information Event Management (SIEM), making the world and its data more efficient and secure. Built by practitioners with the practitioner in mind, Graylog unlocks answers from data for thousands of IT and security professionals who solve security, compliance, operational, and DevOps issues every day. Deployed in more than 50,000 installations worldwide, Graylog is an award-winning platform built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. Graylog eliminates the noise and delivers an exceptional user experience by making data analysis, threat hunting, detection, and incident investigation fast and efficient using a more cost-effective and flexible architecture.

www.graylog.org
info@graylog.com
1301 Fannin Street, Suite 2000
Houston, TX 77002

APPENDIX A: CONTROLS

General Requirement	CIS Controls v.7.1	NIST 800-53	ISO 27001:2013
Identity and Access Management	**Control 1: Inventory and Control of Hardware Assets** Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access. **Control 14: Controlled Access Based on the Need to Know** The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. **CIS Control 16: Account Monitoring and Control** Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.	**AC-1:** Develop, document, and disseminate access control policy. **AC-2:** Define and document the types of accounts allowed and specify prohibited within the system. Specify authorized users, group and role membership, and access authorizations. Monitor use of accounts. **IA-2:** Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users. **IA-3:** Uniquely identify and authenticate organization-defined devices and/or types of devices before establishing a local, remote, or network connection.	**A.9.1.1:** An access control policy shall be established, documented and reviewed based on business and information security requirements. **A.9.2.1:** User access management to ensure authorized user access and to prevent unauthorized access to systems and services. **A.9.4.1:** Information access restriction occurring to access control policy. **A.9:** Access Control. **A.9.1.1:** Access control policy. **A.9.1.2:** Access to networks and network services. **A.9.3.1:** use of secret authentication information. **A.9.4.1:** information access restriction.
Configuration Management	**Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches** Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	**CM-1:** Develop, document, and disseminate configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls.	
Information Security Program		**PM-1:** Develop and disseminate an organization-wide information security program plan that provides an overview of requirements, description of management and common controls, identification of roles and responsibilities across the organization, reflects coordination among organizational entities responsible, and has senior management approval. **SC-1:** Develop, document, and disseminate a system and communications protection policy that identifies purpose, scope, roles, and responsibilities that is also consistent with compliance requirements. The policy should also include procedures to facilitate implementation and protection controls.	**A.5.1.1:** Policies for information security: A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties. **A.6.1.5:** Information security in project management: Information security shall be addressed in project management, regardless of the type of the project.

APPENDIX A: CONTROLS

General Requirement	CIS Controls v.7.1	NIST 800-53	ISO 27001:2013
Continuous Vulnerability Monitoring	**Control 3: Continuous Vulnerability Management** Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.		**A.12.6:** Prevent the exploitation of technical vulnerabilities.
Incident Detection and Response	**CIS Control 19: Incident Response and Management** Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.	**SI-1:** Develop, document, and disseminate a system and data integrity policy that identifies purpose, scope, roles, and responsibilities that is also consistent with compliance requirements. The policy should also include procedures to facilitate implementation and protection controls.	**A.12.2.1:** Controls against malware: Establish detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user Awareness. **A.16.1.1:** Responsibilities and procedures: Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

APPENDIX B: EVENT LOGS

General Requirement	CIS Controls v.7.1	NIST 800-53	ISO 27001:2013
Audit and Accountability	**6.1:** Utilize three synchronized time sources: Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent. **6.2:** Activate audit logging: Ensure that local logging has been enabled on all systems and networking devices. **6.3:** Enable detailed logging: Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	**AU-2:** Event logging: Event logging also supports specific monitoring and auditing needs. Event types include password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage.	**A.12.4.1:** Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed. System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
Identity and Access Management	**1.3:** Use DHCP Logging to Update Asset Inventory: Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory. **4.8:** Log and Alert on Changes to Administrative Group Membership: Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges. **4.9:** Log and Alert on Unsuccessful Administrative Account Login: Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account. **14.9:** Enforce Detail Logging for Access or Changes to Sensitive Data: Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring). **15.2:** Detect Wireless Access Points Connected to the Wired Network: Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network. **16.12:** Monitor Attempts to Access Deactivated Accounts: Monitor attempts to access deactivated accounts through audit logging. **16.13:** Alert on Account Login Behavior Deviation: Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.	**AC-2(4):** Automatically audit account creation, modification, enabling, disabling, and removal actions. **AC-2 (12)(b):** Report atypical usage of system accounts. **AC-6(9):** Log the execution of privileged functions. **AC-7:** Enforce a limit of consecutive invalid logon attempts by a user. **AC-17(1):** Employ automated mechanisms to monitor and control remote access methods. **IA-3(3.b):** Audit dynamic address allocation lease information and duration when assigned to a device. **MP-4(2):** Restrict access to media storage areas and log access attempts and access granted.	**A.6.2.1:** Mobile device policy: A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices. **A.6.2.2:** Teleworking: A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking Sites. **A.8.3.3:** Physical media transfer: Media containing information shall be protected against unauthorized access, misuse or corruption during transportation. **A.9.1.2:** Access to networks and network services: Users shall only be provided with access to the network and network services that they have been specifically authorized to use. **A.9.2.4:** Management of secret authentication information of users: The allocation of secret authentication information shall be controlled through a formal management process. **A.12.4.1:** Event logging: recording user activities, exceptions, faults and information security events shall be produced, kept, and regularly reviewed. **A.12.4.3:** Administrator and operator logs: System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

APPENDIX B: EVENT LOGS

General Requirement	CIS Controls v.7.1	NIST 800-53	ISO 27001:2013
Configuration and Change Management	**5.5:** Implement Automated Configuration Monitoring Systems: Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur. **11.2:** Document Traffic Configuration Rules: All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.	**CM-3(f):** Monitor and review activities associated with configuration-controlled changes to the system. **CM-5(1):** (a)Enforce access restrictions using organization-defined automated mechanisms; and (b) Automatically generate audit records of the enforcement actions.	**A.12.1.2:** Change management: Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.
Continuous Vulnerability Monitoring	**3.1:** Run automated vulnerability scanning tools: Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems. **3.2:** Perform authenticated vulnerability scanning: Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested. **3.6:** Compare Back-to-Back Vulnerability Scans: Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner. **3.7:** Utilize a risk-rating process: Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities. **12.6:** Deploy Network-Based IDS Sensors: Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries. **13.3:** Monitor and Block Unauthorized Network Traffic: Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	**PM-31(c, d, e):** Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy, correlation and analysis of information generated by control assessments and monitoring, and response actions to address results of the analysis of control assessment and monitoring information. **RA-5 (a, b, d):** Monitor and scan for system and application vulnerabilities. Employ vulnerability monitoring tools and techniques by using standards for enumerating platforms, software flaws, and improper configurations, and measuring vulnerability impact. Remediate legitimate vulnerabilities within organization-defined response times. **RA-6:** Employ a technical surveillance countermeasures survey at organization-defined locations using organization-defined frequency when the organization-defined events or indicators occur.	**A.12.6.1:** Management of technical vulnerabilities: Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

APPENDIX B: EVENT LOGS

General Requirement	CIS Controls v.7.1	NIST 800–53	ISO 27001:2013
System Communications and Protection	**2.7:** Utilize application whitelisting: Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets. **2.8:** Implement application whitelisting of libraries: The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process. **2.9:** Implement application whitelisting of scripts: The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1,*.py, macros, etc.) are allowed to run on a system. **7.6:** Log All URL Requests: Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems. **9.5:** Implement Application Firewalls: Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged. **12.2:** Scan for Unauthorized Connections Across Trusted Network Boundaries: Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary. **12.5:** Configure Monitoring Systems to Record Network Packets: Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	**SC-7(9)(a, b):** Detect and deny outgoing communications traffic posing a threat to external systems; and audit the identity of internal users associated with denied communications. **SC-7(15):** Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing. **SC-7(24)(a, b, c, d):** For systems that process personally identifiable information: Apply the organization-defined processing rules to data elements of personally identifiable information; Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system; Document each processing exception; and Review and remove exceptions that are no longer supported.	**A.13.1.1:** Networks shall be managed and controlled to protect information in systems and applications. **A.13.1.2:** Security of network services: Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced. **A.14.1.2:** Securing application services on public networks: Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. **A.14.1.3:** Protecting applications services transactions: Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

APPENDIX B: EVENT LOGS

General Requirement	CIS Controls v.7.1	NIST 800-53	ISO 27001:2013
Incident Detection and Response	**8.6:** Centralize Anti-Malware Logging: Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting. **8.7:** Enable DNS Query Logging: Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains. **8.8:** Enable Command-Line Audit Logging: Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash. **12.8:** Deploy Network-Based Intrusion Prevention Systems: Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries. **15.3:** Use a Wireless Intrusion Detection System: Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network. **15.10:** Create Separate Wireless Network for Personal and Untrusted Devices: Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly. **19.8:** Create Incident Scoring and Prioritization Schema: Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.	**SI-3(8):** Detect unauthorized commands to critical interfaces through the kernel application programming interface, including with virtual machines and privileged applications. Set detection to either issue a warning, audit the command execution, or percent the command execution. **SI-4(22):** Monitor the system to detect attacks and indicators of potential attacks and unauthorized local, network, and remote connections. Detect network services that have not been authorized or approved then set alert as either Audit or Alert when detected. **SI-7(8):** Employ integrity verification tools to detect unauthorized changes to software, firmware, and information. If a potential integrity violation is detected, audit the event and generate an audit record, alert current user, and/or alert responsible party.	**A.16.1.2:** Reporting information security events: Information security events shall be reported through appropriate management channels as quickly as possible. **A.16.1.3:** Reporting information security weaknesses: Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services. **A.16.1.4:** Assessment of and decision on information security events: Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents. **A.16.1.5:** Response to information security incidents: Information security incidents shall be responded to in accordance with the documented procedures. **A.16.1.7:** Collection of evidence: The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

APPENDIX C: REPORT REVIEWS

CIS Controls v.7.1	NIST 800-53	ISO 27001:2013
6.5: Central log management: Ensure that appropriate logs are being aggregated to a central log management system for analysis and review. **6.7:** Regularly review logs: On a regular basis, review logs to identify anomalies or abnormal events. **6.8:** Regularly tune SIEM: On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	**AU-2:** Event logging: Reviewing and updating the set of logged events is necessary to help ensure that the events remain relevant and continue to support the needs of the organization.	**A.18.2.3:** Technical Compliance Review: Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.