



How QRadar Addresses Regulatory Compliance Requirements

Rationalizing Compliance Requirements Amid the Hype

Overview

If you are reading this white paper, you are probably researching how to respond to compliance-driven IT security requirements placed on your organization by management, third-party consultants, or internal and external auditors. These requirements typically involve demonstrating specific security controls that align with internal corporate policies or external government regulations that are specific to your vertical market or type of business (HIPAA, GLBA, PCI, FISMA, NERC-CIP and SOX are some examples).

While it is hard to imagine a more over-hyped market driver than compliance, the requirements placed on you are real and you must respond. The frustrating part of this exercise is the lack of hard and fast guidelines about what really constitutes compliance with a policy or regulation. Gartner provides the most realistic and, at the same time, concerning, evaluation of the compliance dilemma.

“The secret is that there is no definitive assertion of what equals compliance, so organizations are on their own to determine what is reasonable and appropriate for them.”

Chief Information Security Officer’s Guide to Compliance,
Gartner Group, January 2006

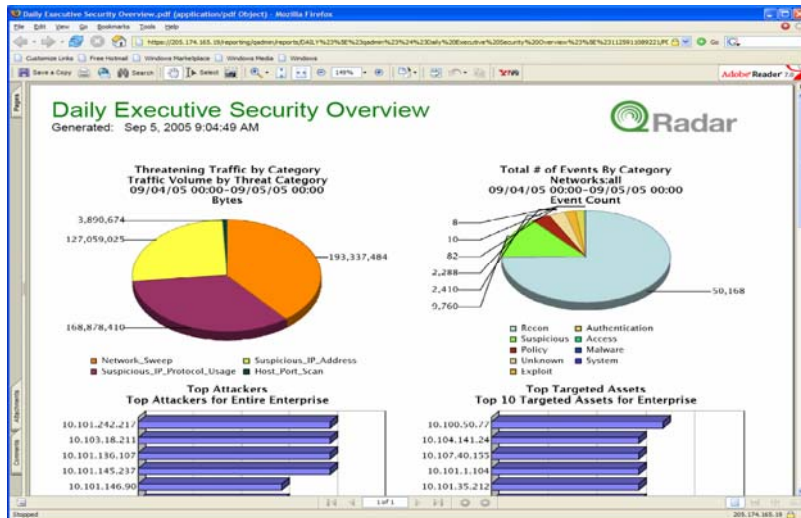
Recognizing that compliance with a policy or regulation often works on a sliding scale, Gartner and others assert that demonstration of, or support for, compliance should involve these key factors:

- **Accountability:** Proving surveillance to report on who did what and when
- **Transparency:** Providing visibility into the security controls, the business applications and the assets that are being protected
- **Measurability:** Metrics and reporting around IT risks within a company

Although no magical tool exists to enable compliance, monitoring and management solutions that span the network and security technologies in your environment play a key part in supporting your various policy initiatives. The intent of this white paper is to rationally depict the value that QRadar Network Security Management brings to enterprises, institutions and agencies for establishing a comprehensive IT security program as part of a compliance initiative.

QRadar Supports Corporate Compliance Initiatives

QRadar provides key technology underpinnings for a company's efforts to enforce accountability, transparency and measurability for supporting its policy and regulatory requirements.

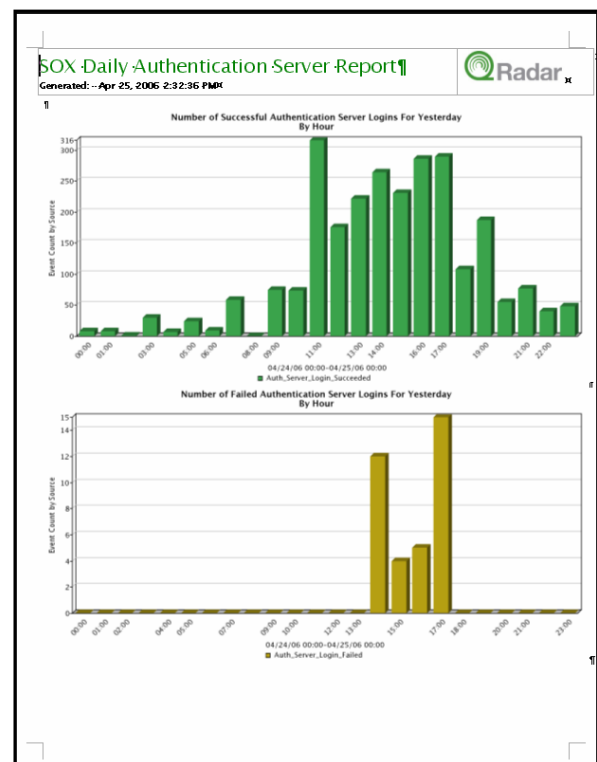


Accountability: Key to a compliance initiative is QRadar's broad management of relevant network, security, host and application information across the entire IT infrastructure. While many technologies can monitor events from different security and other device platforms, only QRadar provides the added benefit of a real-time and historical look into network and application behavior. These two very important sets of information combine to generate a broad operational span for enforcing accountability. Correlating network data with security information yields a more accurate picture of network and user activity and provides greater forensic granularity for investigating compliance violations.

Transparency: Visibility into security controls is clearly one of the primary functions of a security monitoring and management platform like QRadar. Of even greater importance is QRadar's ability to look not only at the security devices but also into the application traffic on the network so as to assess business relevance and the traffic's compliance with corporate policy. QRadar also natively builds profiles of all the assets on the network that can and should be grouped by business function (e.g. servers that are subject to SOX compliance audits). You can assign a business value to these asset groups so you can appropriately weight by risk the network and security information that pertains to them.

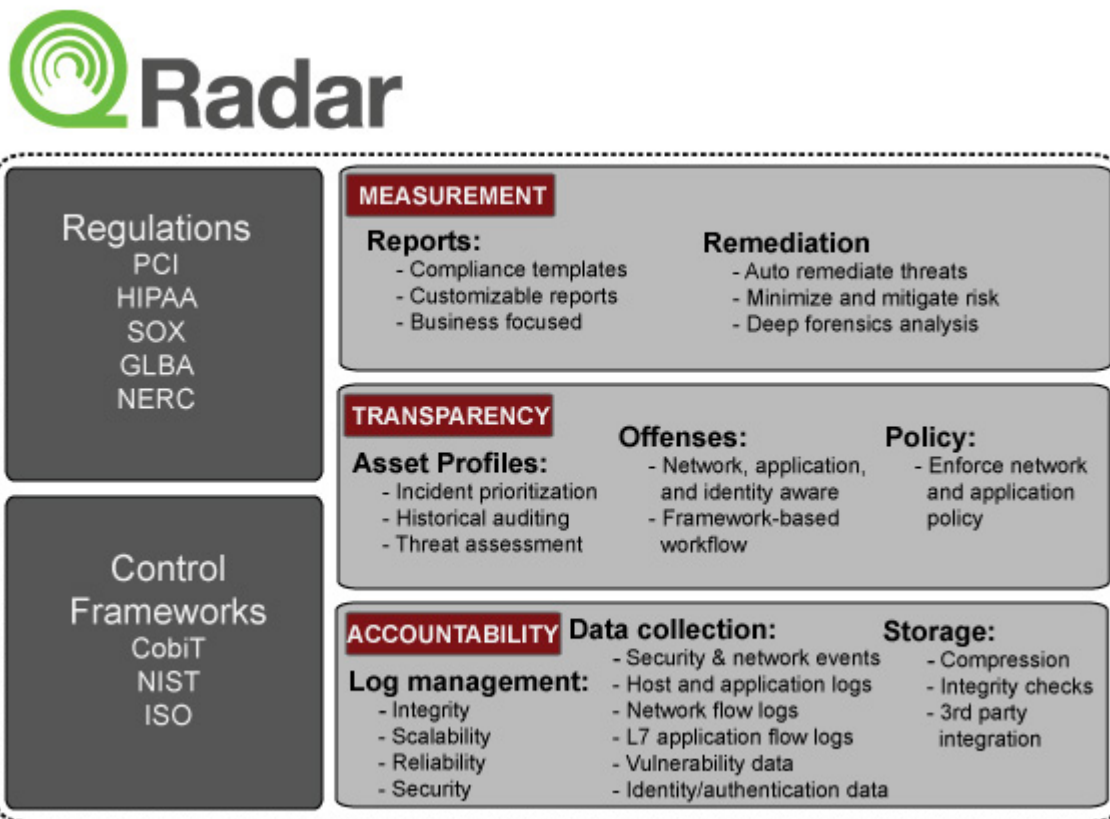
Measurability: The metrics for assessing or measuring compliance are provided through QRadar's interactive dashboards and reporting. The dashboards are critical for monitoring real-time awareness and response to compliance and policy violations. QRadar reports supply the supporting information that is required periodically by internal and external auditors to demonstrate compliance with regulations.

QRadar provides a set of default compliance-focused reports and rules based on industry control frameworks and applied specific regulations. These give you a great starting point but, as auditor requirements may change frequently, note that you can get equal value from the product's flexible rule and custom report-generating engines.



to

Features in QRadar that directly support compliance initiatives



Because achieving compliance is more than simply generating reports, it is necessary to look at all the technology underpinnings that support a company's compliance initiatives.

Features supporting accountability

From an accountability perspective, QRadar collects an unrivaled set of surveillance data and provides a log management solution optimized for long-term storage needs. Specific features in QRadar that provide accountability include:

- **Events and logs:** QRadar collects events and logs from a heterogeneous set of sources that includes network infrastructure, security devices, servers, operating systems and applications. It normalizes all events to enable automatic out-of-box correlation with other events and network flows. To meet specific compliance requirements logs can be stored in their original raw format. In addition to event data, QRadar also gathers vulnerability data to incorporate in asset profiles (See Asset Profiles) that are maintained for each business asset.
- **Network flows:** QRadar surveys the entire network, using native flow sources in a customer's routing/switching infrastructure or from distributed collectors to gather a detailed history of all network flow activity. All observed network flows are analyzed to build behavioral models that capture network behavior and to generate alerts when anomalous behavior is detected.

- **Storage:** QRadar stores all the raw events and flows that it collects to enable detailed forensics and compliance reporting. Storage from 0.5TB to 44TB has been tested with QRadar systems. Retention settings of graphical, forensic and event data can be adjusted by the user to his requirements. A custom store eliminates the need for the secondary software costs and ongoing maintenance costs that plague other offerings. Designed specifically for the storage, retrieval, and analytics of network flow data, the QRadar store is vastly more efficient than off-the-shelf databases that are ill-suited for the task of storing security event and network flow management.
- **Data Integrity:** The security of communications (configuration data as well as monitored and analyzed data) between QRadar appliances is protected through encrypted tunnels. To guarantee that log files have not been tampered with QRadar implements extensive log file integrity checks, including NIST Log Management Standard SHA-x (1-256) hashing algorithms. QRadar also provides an additional layer of encryption options for customers requiring additional levels of file integrity including federal customers wishing to comply with FIPS 140-2 encryption requirements

Features supporting transparency

QRadar provides visibility into the security controls and assets/applications being protected through powerful analytics that provide knowledge required for key compliance controls. Specific features in QRadar that provide transparency include:

- **Asset Profiles:** QRadar passively monitors network activity and builds real-time profiles of all network assets. It automatically measures risk exposure by augmenting these asset profiles with asset vulnerability and activity data gathered from third-party vulnerability scanners deployed within the same network. QRadar asset profiles identify business assets that are at risk of attack, not just those that are already under attack. As QRadar automatically builds these profiles from IPs appearing on the network, administrators have the ability to group and weight the importance of the assets and this weighting is used to determine a security event's priority when it occurs. Assets maintain a historical perspective of user and system identity associated with the asset. Assets can be named and grouped by specific regulations (e.g. "PCI Servers") for improved compliance management. This lets the QRadar administrator view any asset within the network and get a picture of that resource.
- **Offenses:** QRadar offenses bring together the security events, user identity, asset profiles/vulnerabilities and traffic flows, relating them to policy violations, misuse and threats to your business. Offenses are a complete record of all security events, network transactions and additional contextual information (derived from correlation tests) observed during an attack or violation. With QRadar, default correlation rules will create an offense if certain security controls are violated. Customer-specific policy rules are easily created using the QRadar rules engine.(e.g. Following NIST 800-53 AC-7, QRadar will create an offense if an IP address is observed to have multiple failed login attempts against specific servers and then followed by a successful login.)
- **Application Visibility:** QRadar analyzes network activity to identify applications. This allows for a granular view of application communications, enabling very specific compliance policies, malware identification and profiling of network usage. QRadar can also capture a portion of the content for each flow that is being observed. A configurable amount of content can be stored from the start of each flow which provides unrivaled forensic capabilities when investigating compliance issues.

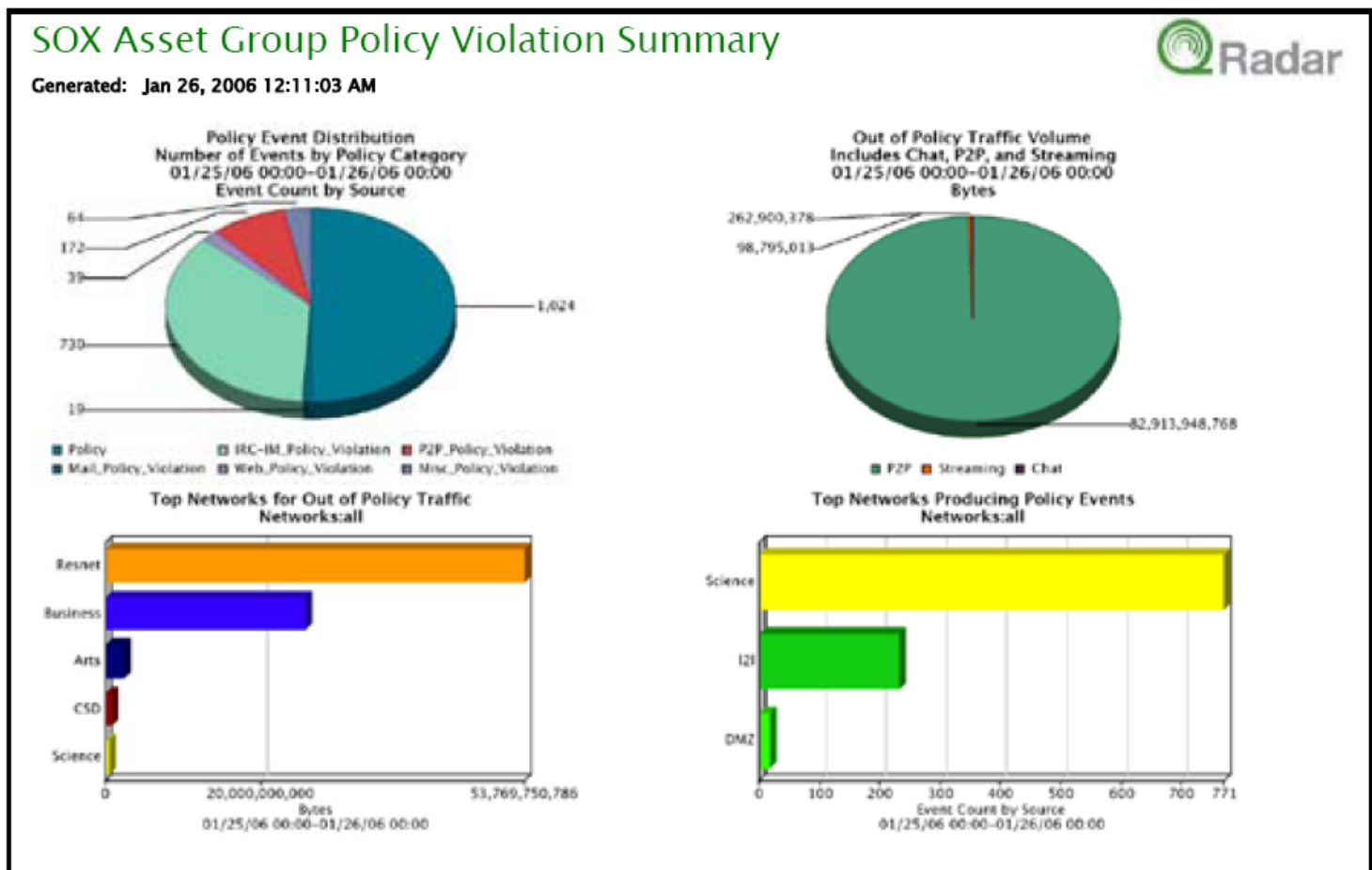
An overview of specific compliance monitoring filters can be found in Appendix A.

Features supporting measurability

Finally, QRadar provides regulation and control specific features including:

- **Reports:** QRadar offers a robust reporting engine providing users with the capability to quickly and easily create customized reports for the critical business assets that are most important to them. Reports can be created for any portion of the network and most any measure taken by QRadar. Default compliance-focused reports and rules based on industry control frameworks can be applied for specific regulations.
- **Remediation:** Once a violation is understood, QRadar leverages the most appropriate security device or component of the network infrastructure to resolve them. It offers multiple options for remediation so you can fix the problem from your console, applying the most effective method to resolve the compliance issue.

An overview of specific compliance reports can be found in Appendix B.



Control Frameworks Reflected in QRadar Functionality

Regulatory compliance is driving many IT organizations to adopt frameworks for managing compliance and its accompanying controls. While magazine articles, peer conversations and marketing literature often focus on the regulation itself, the means of actually achieving compliance lies in how successfully you implement one of several control frameworks.

In many cases you can map a control framework directly to a regulation. For example, CobiT controls map directly to the security requirements within Sarbanes Oxley and NIST controls map directly to the security requirements within FISMA.

QRadar contains specific controls (reports, alerts or asset groupings) specified by CobiT, NIST and ISO that address the key areas of these control frameworks that must be met by a network security management platform.

A summary of security controls supported by QRadar for specific regulations and security best practices can be found in Appendix A.

Summary

Recognizing that compliance with a policy or regulation often works on a sliding scale, Gartner and others assert that demonstration of, or support for, compliance initiatives should involve these key factors:

- **Accountability:** Proving who did what and when
- **Transparency:** Providing visibility into the security controls, the business applications and the assets that are being protected
- **Measurability:** Metrics and reporting around risk within a company

Customers leverage QRadar to deliver the accountability, transparency and measurability required to meet security management best practices and support compliance initiatives including CobiT, ISO 17799, Payment Card Industry-Data Security Standard (PCI-DSS), Sarbanes-Oxley (SOX), Graham-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and North American Electric Reliability Corp Critical Infrastructure Protection (NERC CIP). A summary of specific areas supported by QRadar for each of these regulations can be found in Appendix C

Appendix A: Regulatory and IT best practices supported by QRadar

Regulation/Best Practice	Industry Represented	Requirement
Payment Card Industry Data Security Standard (PCI-DSS)	Retail/Finance	<p>Most major credit card providers, including Visa and Mastercard, are now mandating that any merchant and service provider that deals with credit card holder information must implement a security program that complies with the Payment Card Industry Data Security Standard (PCI-DSS).</p> <p>Specific security control areas provided by PCI-DSS that are supported by QRadar's log and security management capability include:</p> <ul style="list-style-type: none"> ➤ Maintaining & building a secure network ➤ Protecting card holder data ➤ Maintaining a vulnerability assessment program ➤ Implementing strong access controls ➤ Regularly monitoring and testing networks ➤ Maintaining an information security policy <p>For more information on how QRadar assists in meeting PCI-DSS, please read the whitepaper titled "<i>Meeting PCI data security standards with QRadar network security management</i>"</p>
Health Insurance Portability and Accountability Act (HIPAA)	Healthcare	<p>The health care industry is now under the federal mandates of HIPAA and the "Security Standards for the Protection of Electronic Protected Health Information"</p> <p>Specific security control objectives dictated by HIPAA that are supported by QRadar's log and security management capability include:</p> <ul style="list-style-type: none"> ➤ Reduce vulnerabilities

		<p>(164.308(a)(1)(ii)(B))</p> <ul style="list-style-type: none"> ➤ Information system activity review (164.308(a)(1)(ii)(D)) ➤ Protection from malicious software (164.308(a)(5)(ii)(B)) ➤ Log-in monitoring (164.308(a)(5)(ii)(C)) ➤ Security incident response and reporting 164.308(a)(6)(ii) ➤ Audit controls (164.312(b)) ➤ Integrity of records (164.312(c)(1))
<p>Sarbanes-Oxley (SOX)</p>	<p>Public Companies</p>	<p>Section 404 of SOX specifies that an annual report must be delivered that</p> <ol style="list-style-type: none"> 1. states the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and 2. contains an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal controls. <p>In addition, it mandates an external audit of the procedures used to deliver the report.</p> <p>Although the SOX requirements are relatively broad, organizations under the scrutiny of the regulation must implement an information security program to protect the integrity of financial reports. Any prudent information security program will require a log management framework like the one provided by QRadar.</p> <p>SOX driven security management programs will typically follow a well defined set of control objectives, like CobiT, that require more than just basic log management. There are many important CobiT control objectives supported by QRadar including monitoring and reporting to ensure system security. More detail on this is covered below in the CobiT section of this table.</p>

		In addition, section 802 of SOX requires supporting materials used in the delivery of the financial reports must be maintained unaltered for 5 years. QRadar's log management capability enables organizations to efficiently and securely manage logs for an extended period of time.
Gramm-Leach-Bliley Act (GLBA)	Financial Institutions	<p>GLBA was enacted by congress and mandates that financial organizations "protect the security, integrity and confidentiality of consumer information. Section 501(b) of GLBA states that organizations must "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards--</p> <p>(1) to insure the security and confidentiality of customer records and information;</p> <p>(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and</p> <p>(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer"</p> <p>GLBA driven security management programs will typically follow a well defined set of control objectives, like CobiT, that requires more than just basic log management. There are many important CobiT control objectives supported by QRadar including monitoring and reporting to ensure system security. More detail on this is covered below in the CobiT section of this table.</p>
National Institute of Standards & Technology (NIST) North American Electric Reliability	Utilities Manufacturing	The control systems that manage the delivery of utilities (i.e. gas, electricity, water, etc.) and support manufacturing processes are increasingly being scrutinized because of their vulnerability to cyber-terrorism.

<p>Corp (NERC) Critical Infrastructure Protection (CIP) Federal Energy Regulatory Commission (FERC)</p>		<p>There are many different control systems, including supervisory control & data acquisition systems (SCADA), that are extremely susceptible to vulnerabilities because of deficiencies in the architectures that have evolved over many years.</p> <p>With increased use of off-the-shelf server technologies in control systems, concern over potential vulnerabilities has increased. This has resulted in emerging security best practices and regulations focused on tightening security for control systems that, if compromised, could cause a catastrophe.</p> <p>Multiple standards have emerged including the NERC Cyber Security Standards for Critical Information Protection (CIP) that outlines 8 areas of security control:</p> <p>Specific security control objectives dictated by NERC CIP that are supported by QRadar's log and security management capability include:</p> <ul style="list-style-type: none"> ➤ (CIP-001-1) Sabotage Reporting ➤ (CIP-002-1) Critical Cyber Asset Identification ➤ (CIP-003-1) Security Management Controls ➤ (CIP-005-1) Electronic Security Perimeter(s) ➤ (CIP-007-1) Systems Security Management ➤ (CIP-008-1) Incident Reporting and Response Planning
<p>Federal Information Security Management Act (FISMA)</p>	<p>Government</p>	<p>FISMA was enacted in 2002 to ensure the integrity of government IT systems. The regulation mandates specific security controls that must be implemented by all federal government agencies and all contractors or other businesses that provide IT based services to federal agencies.</p>

		<p>A key requirement of FISMA is the implementation of an acceptable set of security controls that are defined by:</p> <ul style="list-style-type: none"> ➤ Federal Information Processing Standards (FIPS) ➤ NIST special publication 800-53; “Recommended security controls for federal information systems” <p>There are many important control objectives defined in these guidelines supported by QRadar including monitoring and reporting to ensure system security. More detail on this is covered below in the FIPS and Special Publication 800-53 section of this table.</p>
CobiT	All	<p>There are multiple areas of CobiT that specify that optimal security is only achieved through “an organization wide continuous improvement program that takes into account lessons learned and industry best practices for internal control monitoring” (ME2: Monitor and Evaluate Internal Controls).</p> <p>Specific security control objectives dictated by CobiT that are supported by QRadar’s log and security management capability include:</p> <ul style="list-style-type: none"> ➤ DS3 – Manage Performance & Capacity ➤ DS4 – Ensure Continuous Service ➤ DS5 – Ensure Systems Security ➤ DS6 – Identify and Allocate Costs ➤ DS8- Manage Service Desk & Incidents ➤ DS9 – Manage the Configuration ➤ DS10 – Manage Problems ➤ ME1 – Monitor and Evaluate IT Performance ➤ ME2 – Monitor and Evaluate Internal Control ➤ ME3 – Ensure Regulatory

		<p>Compliance</p> <ul style="list-style-type: none"> ➤ ME4 – Provide IT Governance
<p>ISO 17799 Information technology- Security techniques – Code of practice for information management</p>	<p>All</p>	<p>Similar to CobiT, many areas of ISO 17799 benefit from a log and security management solution like QRadar.</p> <p>Specific security control objectives dictated by ISO 17799 that are supported by QRadar’s log and security management capability include:</p> <ul style="list-style-type: none"> ➤ Section 5 - Defining a security policy ➤ Section 7 – Asset management <ul style="list-style-type: none"> ○ 7.1.1 Discovery and inventory of assets ○ 7.1.3 Acceptable use of assets ○ 7.2.1 Classification guidelines ➤ 10 Communications and operations management <ul style="list-style-type: none"> ○ 10.1.3 Segregation of duties ○ 10.4.1 Protection against malicious code ○ 10.6 Network security management ○ 10.6.1 Network controls ○ 10.8.1 Information exchange policies and procedures ○ 10.8.5 Business information systems ○ 10.10 Monitoring <ul style="list-style-type: none"> ○ 10.10.1 Audit logging ○ 10.10.2 Monitoring system use ○ 10.10.3 Protection of log information ○ 10.10.4 Administrator and operator logs ○ 10.10.5 Fault logging ➤ 11.1.1 Access control policy ➤ 11.5.1 Secure log-on procedures ➤ 12.6.1 Control of technical vulnerabilities ➤ 13.1.1 Reporting information security events and weaknesses ➤ 13.2 Management of information security incidents

<p>FIPS 200 & NIST special publication 800-53 revision 1 <i>“Recommended Security Controls for Federal Information Systems”</i></p>	<p>Government</p>	<p>➤ 13.2.3 Collection of evidence</p> <p>Federal Information Processing Standards (FIPS) Publication 200 provides “Minimum Security Requirements for Federal Information and Information Systems”</p> <p>Specific security control areas defined by FIPS 200 that are supported by QRadar’s log and security management capability include:</p> <p>Access Control (AC): “Organizations must limit information system access to authorized users”</p> <p>Audit and Accountability (AU): “Organizations must (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity”</p> <p>Certification, Accreditation, and Security Assessments (CA): “Organizations must: (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.”</p> <p>Incident Response (IR): “Organizations must: (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.”</p> <p>Risk Assessment (RA): “Organizations must periodically assess the risk to organizational operations.”</p> <p>System and Information Integrity (SI): Organizations must: “(ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.”</p>
--	-------------------	---

