

# FISMA: Securing National Infrastructure

---

## Using a Holistic Approach to Lower Total Cost of Ownership (TCO) of FISMA Compliance by 50% or More

an eIQnetworks White Paper

by John Linkous  
*Security and Compliance Evangelist*  
*eIQnetworks, Inc.*



**eIQnetworks**  
31 Nagog Park  
Acton, MA 01720  
t. +1 978.266.9933  
f. +1 978.266.0004  
[www.eIQnetworks.com](http://www.eIQnetworks.com)

© 2010, eIQnetworks, Inc. eIQnetworks, the eIQnetworks logo and SecureVue are registered trademarks of eIQnetworks, Inc. All other trademarks, servicemarks, registered trademarks or registered servicemarks are the property of their respective owners. All rights reserved.

## Contents

<b>Abstract</b>	<b>3</b>
<b>The Business Problem</b>	<b>3</b>
<b>Meeting FISMA Automation and Reporting Challenges</b>	<b>5</b>
<b>The Traditional Approach: Security Point Products</b>	<b>5</b>
Product 1: SIEM and Log Management	6
Product 2: Configuration Auditing and Assessment	6
Product 3: Network Behavioral Analysis (NBA)	6
Product 4: File Integrity Monitoring (FIM)	6
<b>The Integrated Solution Approach: Unified Threat and Compliance (UTC)</b>	<b>6</b>
<b>Integrated Solution (SecureVue) Profile</b>	<b>7</b>
<b>Calculating the Real TCO for FISMA Compliance</b>	<b>8</b>
<b>Assumptions</b>	<b>8</b>
<b>Product Procurement Costs</b>	<b>9</b>
<b>Annual Support and Maintenance Costs</b>	<b>10</b>
<b>Training Costs</b>	<b>11</b>
<b>Professional Services</b>	<b>11</b>
<b>Operations Personnel</b>	<b>12</b>
<b>Conclusion</b>	<b>13</b>
<b>Cost Comparison Table</b>	<b>13</b>
<b>Cost Comparison Charts</b>	<b>13</b>
<b>Appendix 'A': Detail of Security Data Type by NIST 800-53 Control Category</b>	<b>16</b>

## Abstract

As the most broad-based information security standard for federal agencies in the United States, the Federal Information Security Management Act (FISMA) defines a framework of information security risk management, processes, and technical controls that are mandatory for every federal agency, as well as a many private industry organizations that conduct business in partnership with the federal government.

The traditional approach to FISMA compliance requires both technology-based tools to collect relevant FISMA-related security data, as well as processes, oversight and management. While there is no such thing as fully-automated “turnkey” FISMA compliance, a large number of the FISMA requirements can be automated through security tools, reducing the amount of time required to manually address these security processes and controls. Automating FISMA requires implementing key technologies that provide collection and analysis of security-related data; although there are many different types of technologies that can be used to address FISMA automation, the solutions that yield the most comprehensive automation footprint include log management (or SIEM), configuration auditing, vulnerability assessment, and network traffic analysis products. By implementing these solutions - almost always implemented as a series of disparate technologies, often from different vendors - organizations can achieve significant automation and reporting for FISMA compliance. **However, by taking a different approach based on a single, integrated platform that brings together all relevant FISMA data for automation and reporting, the total cost of ownership (TCO) for FISMA compliance can be reduced by 50% or more over a three-year period.**

In this white paper, eIQnetworks documents the true TCO associated with the traditional method of FISMA compliance, and compares this approach to one based on eIQnetworks’ SecureVue solution. Individual cost factors between both solutions are compared in a typical FISMA compliance scenario, and a comprehensive summary comparison identifies the real-world costs associated with both approaches.

## The Business Problem

As a U.S. federal law, FISMA by itself does not mandate specific technologies, or even detailed information security controls that must be implemented in support of the law. Instead, FISMA relies on detailed guidance provided through the National Institute of Standards and Technology (NIST), which has established a series of Special Publications (SPs) and Federal Information Processing Standards (FIPS) that can be used by federal agencies to implement specific FISMA-compliant standards.

Chief among the NIST publications related to FISMA is NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations". This standard defines a series of specific risk-based technical, operational and managerial controls that span a broad range of information security concepts such as access control, configuration management, incident response, system and communications protection, and others. The eighteen security control families in NIST 800-53 represent the minimum baseline of information security for federal organizations; they are augmented by additional, system-level controls defined in standards such as the Federal Desktop Core Configuration (FDCC) for Windows XP and Windows Vista, and a variety of platform-specific configurations defined in Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs). Together, NIST 800-53 coupled with additional NIST guidance, the FDCC, and DISA STIGs, form the framework of FISMA compliance for federal agencies and other organizations that must implement and maintain FISMA compliance.

Regardless of the specific NIST, FDCC, and DISA STIG standards implemented by organizations seeking to achieve FISMA compliance, each standard requires a combination of technology, people and processes, driven by proper governance. FISMA compliant organizations must address a broad set of data analysis, data retention and monitoring requirements by measuring, archiving, monitoring, analyzing, and reporting on a broad range of security data from across their technology infrastructure, including asset data, configuration data, log and event data, known vulnerabilities, network flows, file integrity and removable media data, written security policies and manual procedures, and physical security audit results.

Table 1 identifies how each of these types of data map to individual requirements in the key components of FISMA; for a detailed breakdown of NIST 800-53 control categories, see Appendix 'A' at the back of this document:

FISMA Standards and Associated Requirements	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
<b>NIST 800-53</b>								
AC - Access Control	■	■	■	■	-	-	■	-
AT - Awareness and Training	-	-	-	-	-	-	■	-
AU - Audit and Accountability	■	■	■	■	■	■	■	■
CA - Security Assessment and Authorization	■	■	■	■	■	■	■	■
CM - Configuration Management	■	■	-	-	-	■	■	-
CP - Contingency Planning	■	■	■	■	■	■	■	■
IA - Identification and Authentication	■	■	■	■	-	-	■	-
IR - Incident Response	■	■	■	■	■	■	■	■
MA - Maintenance	■	■	■	-	-	-	■	-
MP - Media Protection	■	■	■	-	-	■	■	■
PE - Physical and Environmental Protection	■	■	■	-	-	-	■	■
PL - Planning	-	-	-	-	-	-	■	-
PS - Personnel Security	■	■	■	-	-	-	■	-
RA - Risk Assessment	■	■	■	■	■	■	■	■
SA - Systems and Services Acquisition	■	■	■	-	-	-	■	-
SC - System and Communications Protection	■	■	■	■	■	■	■	■
SI - System and Information Integrity	■	■	■	■	-	■	■	■
PM - Program Management	-	-	-	-	-	-	■	-
<b>Prescriptive System Security Control Standards</b>								
FDCC	■	■	-	-	■	■	-	■
DISA STIGs	■	■	-	-	■	■	-	■

Table 1: Security Data Types Required for FISMA Automation and Reporting

# Meeting FISMA Automation and Reporting Challenges

Federal agencies and other designated organizations that must comply with FISMA need to implement technologies to collect and monitor the key types of information security data identified above. At a minimum, this includes four security functions:

- Security Information and Event Management
- Configuration Auditing
- Network Behavioral Analysis (NBA)
- File Integrity Monitoring (FIM)

Organizations that must address these security functions have adopted one of two approaches: a traditional point solution approach in which multiple security products are deployed, often as a “best of breed” set of tools; or, an integrated solution approach in which a multiple security functions are combined into a single platform. Below we provide an analysis of both methods.

## The Traditional Approach: Security Point Products

In a traditional approach to FISMA compliance, organizations meet FISMA automation and reporting challenges using point products to address specific NIST, FDCC, and DISA requirements, as illustrated in Figure 1, below:

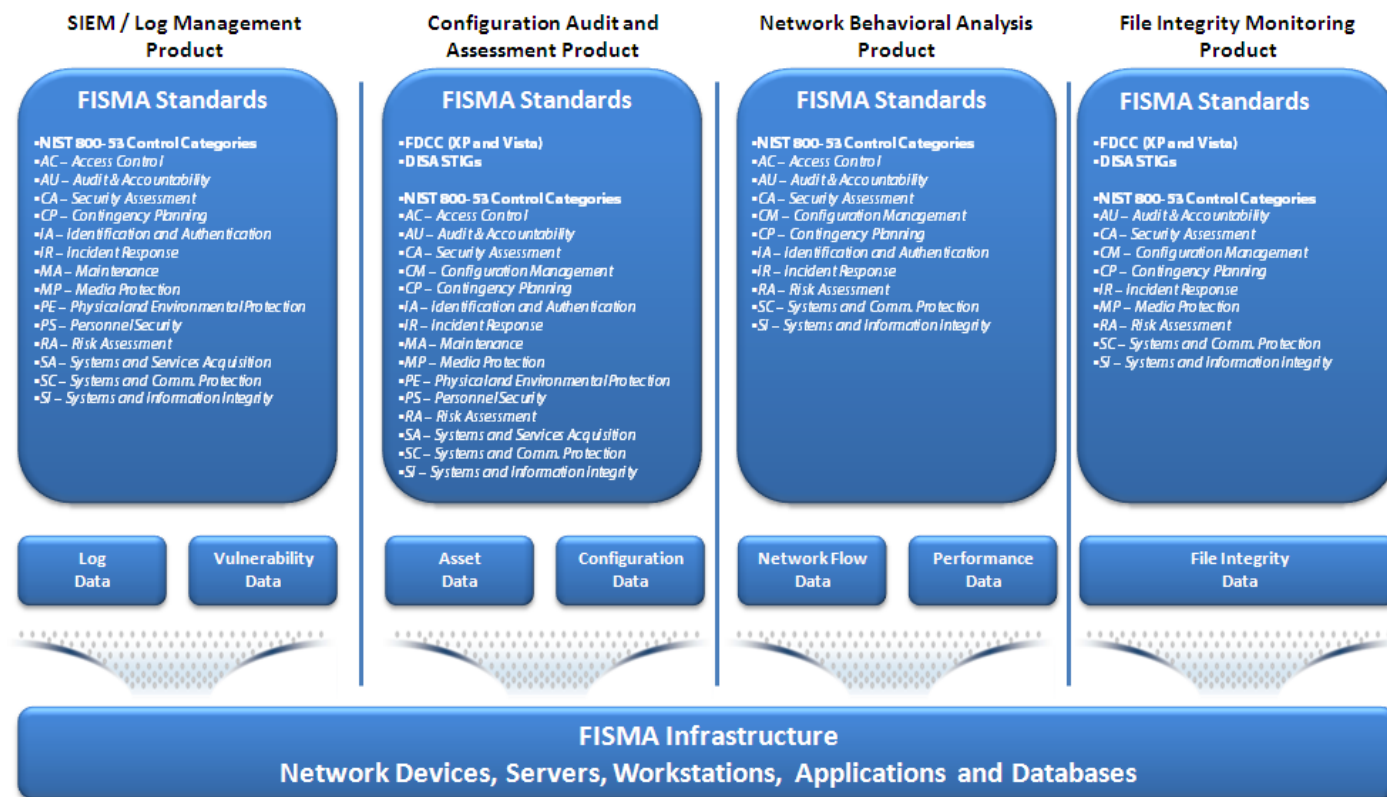


Figure 1: Traditional Approach to FISMA Automation and Reporting

### *Product 1: SIEM and Log Management*

SIEM and log management solutions provide collection, aggregation, and analysis of log and event data from operating systems, network infrastructure devices, security devices, applications, and databases, as well as vulnerability data from third-party scanning products. Common tools that provide this point product functionality include: Arcsight ESM; Q1 Labs Radar; and RSA EnVision. These products partially address a number of NIST 800-53 control categories, but do not fully address any of them. Although SIEM and log management vendors often taut their support for using log data to address prescriptive system-level security standards such as FDCC and DISA STIGs, the reality is that these technologies simply cannot collect actual, current-state configuration data to effectively support them.

### *Product 2: Configuration Auditing and Assessment*

Configuration auditing and assessment products provide the ability to audit secure configurations for systems and applications, and continuously monitor these systems to ensure compliance with these secure baselines. These point solutions capture both what's on a system (such as hardware profile, installed applications, and running services/daemons) as well as how securely these components are configured (such as device settings, password standards, and access control lists). Common tools that provide this point product functionality include: Symantec CCS (formerly BindView); NetIQ Security Manager; and Tripwire Enterprise. These products partially address a number of NIST 800-53 control categories, but do not fully address any of them. They also provide nearly complete support for prescriptive system-level security standards such as FDCC and DISA STIGs.

### *Product 3: Network Behavioral Analysis (NBA)*

NBA security point solutions collect network flow data generated by routers, firewalls, and other network infrastructure devices, analyze this data to determine "normal" traffic patterns, and alert system administrators when normal abnormal network traffic is detected. These products also provide metrics on network data, such as sources and destinations of traffic, as well as network protocols, ports, and applications. Common tools that provide this point product functionality include: Lancope Stealthwatch; and Q1 Labs QRadar. Like other point solutions described in this paper, these products partially address a number of NIST 800-53 control categories, but do not fully address any of them.

### *Product 4: File Integrity Monitoring (FIM)*

FIM products continuously monitor critical files – such as operating system files, files containing sensitive data, and others – using checksum-based data, and immediately notify appropriate personnel when unauthorized or unexpected changes to files and directories occur. Common tools that provide this point product functionality include: TripWire Enterprise; Symantec CCS; and nCircle FIM. Similar to configuration auditing and assessment tools, these products partially address a number of NIST 800-53 control categories (without fully meeting any of them on their own), and also provide support for prescriptive system-level security standards such as FDCC and DISA STIGs.

## **The Integrated Solution Approach: Unified Threat and Compliance (UTC)**

An alternative approach to FISMA compliance provides the same comprehensive coverage of all security data and capabilities (such as alerting and real-time monitoring) as a traditional approach, but provides a significantly lower TCO through both "hard" capitalized costs, as well as operational efficiency. The approach – defined as **unified threat and compliance (UTC)** – provides a single platform that brings together both the operational security requirements and compliance reporting requirements of FISMA standards into a single product. SecureVue from eIQnetworks is a unified threat and compliance solution that meets this more cost-effective alternative approach to addressing FISMA automation and reporting.

## Integrated Solution: SecureVue from eIQnetworks

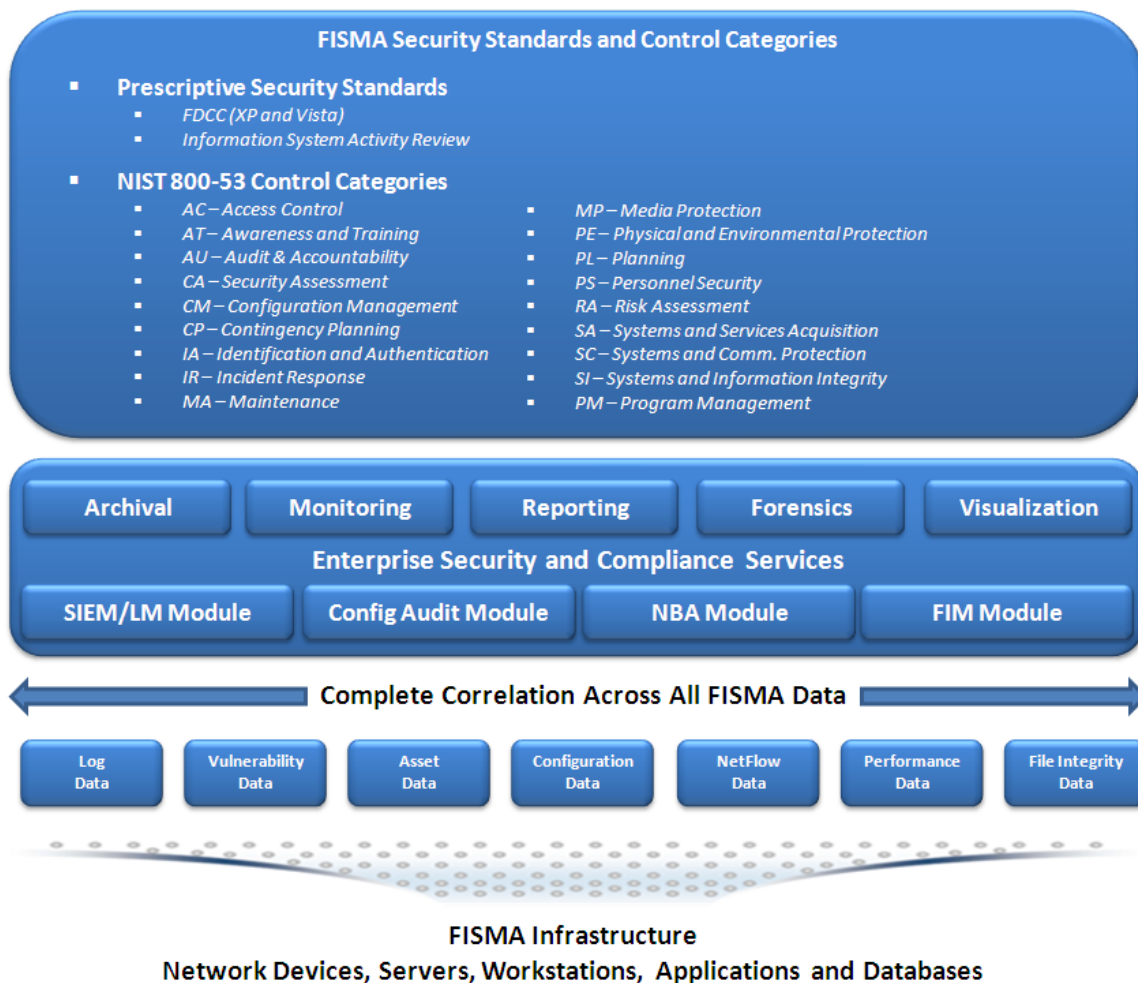


Figure 2: Unified Threat and Compliance (UTC) Approach to FISMA Automation and Reporting

The above diagram illustrates the breadth of collected security data, as well as the depth of security and compliance functions, provided by the SecureVue platform. Using an integrated solution such as SecureVue, federal agencies and other organizations that must address FISMA compliance can automate and report on a broad set of security controls using a single product, without the need to generate piecemeal FISMA compliance reports from different tools or master multiple point products that each provide only a “wedge” of FISMA compliance capability.

### Integrated Solution (SecureVue) Profile

SecureVue from eIQnetworks captures, monitors, correlates, analyzes, and reports on an extremely broad set of security data required to address FISMA compliance, including: log and event data; asset data; configuration data; vulnerability data; performance data; network flow data. SecureVue's breadth of data includes:

- **Log data** from servers, workstations, network devices, applications and databases
- **Vulnerability data** (via a third-party vulnerability scanner) from servers, workstations, network devices and applications

- **Asset data**, such as installed applications and patches, and device/host hardware information, from servers, workstations and network devices. *SecureVue collects this data without the need for an agent.*
- **Security configuration data**, such as password properties and Windows registry settings, from servers, workstations and network devices. *SecureVue collects this data without the need for an agent.*
- **Network flow protocols**, including NetFlow, C-Flow, J-Flow, and others, from network infrastructure and security devices that generate flow data
- **File integrity data** based on both checksums and properties of files and directories
- **Performance data** from multiple sources, including SNMP and a variety of other protocols

Together, this broad set of data coupled with SecureVue's extensive analysis capabilities provide organizations with the most complete single solution available to provide automation and reporting across FISMA-related standards including NIST 800-53, FDCC, and DISA STIGs.

## Calculating the Real TCO for FISMA Compliance

Comparing a traditional security point product approach for FISMA compliance to an approach based on an integrated solution, it's clear that an approach encompassing multiple tools is inefficient. Using the point product approach, collecting all of the data and achieving all of the security functions required for FISMA compliance requires the purchase of multiple security point products.

In this section of the white paper, we will analyze the specific costs associated with both approaches by comparing traditional FISMA security point products against an integrated solution such as eIQnetworks' SecureVue. These specific cost categories include: product procurement costs; support and maintenance costs; training costs; professional services; and operations personnel.

### Assumptions

Calculating TCO for a FISMA compliance solution is, of course, a relative process; specific assumptions must be made about the size and scope of the agency's technology environment, personnel costs, and other highly variable factors. For the TCO analysis presented below, the following assumptions are made that are typical of a mid-size geographic site within a typical United States federal department or agency:

- **Environment Size.** The organization maintains a total of 1,000 nodes. This includes 300 network devices (routers, switches, firewalls, UTM, IDP, DLP, etc.), and 700 servers (Windows, UNIX, Linux, and others).
- **Solution Deployment Hardware.** This paper does not include hardware costs due to the significant range of pricing that is affected dedicated vs. shared hardware, virtualization, and other factors. However, it is safe to assume that it is likely more computing power is required for multiple point solutions, than a single, integrated solution.
- **Software Pricing.** SecureVue pricing is based on the list price of SecureVue, delivered as an appliance (one of several delivery methods for the software). SIEM point solution pricing, configuration auditing product pricing, NBA product pricing, and FIM product pricing are based on the average list price of multiple tools in their respective categories.
- **Maintenance Agreements.** Full maintenance agreements are purchased up-front on software for three (3) years.
- **Maintenance Support Level.** All software updates are included, and live vendor support is provided at least 8x5, with 7x24x365 access to on-line support options provided by the vendor.

- **Maintenance Pricing.** Maintenance costs are assumed to be 20% of the product base license, per year. This is in line with maintenance and assurance agreements throughout the IT industry.
- **Personnel for Product Training.** Two (2) personnel are assumed to be trained on each product.
- **Product Training Pricing.** Pricing for training is based on a typical rate of \$2,500 per day, per trained employee. Training is assumed to take two (2) days per product, and is assumed to take place on-site at the organization (i.e., no additional costs for travel and expenses are assumed).
- **Professional Services Personnel.** The organization uses vendor-provided resources for both deployment architecture design, and implementation services. It is assumed that one (1) vendor-provided resource conducts professional services at a time.
- **Professional Services Pricing.** Pricing for professional services is based on an assumed five (5) days of total professional services required per product: one (1) day for deployment architecture design; and (4) days for implementation services. The baseline daily rate (excluding travel and expenses) for a professional services resource is \$2,500 per day.
- **Operations Personnel Costs.** The fully-loaded cost of the organization’s full-time personnel is \$100,000 per year. This value may vary based on factors such as geographic location and the overall experience of the personnel.
- **Operations Personnel Allocation for Administration.** Based on typical real-world use, this paper assumes that SIEM and integrated solution products each product require one (1) FTE for annual administration and maintenance, while configuration auditing, NBA, and FIM products require a one-half (.5) FTE for the same.
- **Operations Personnel Allocation for DBA.** For products that are back-ended by a commercial relational database management system (RDBMS), this paper assumes that SIEM products require one (1) FTE for annual database administration, while configuration auditing, NBA, and FIM products require a one-half (.5) FTE for the same.

## Product Procurement Costs

The most obvious cost factor when calculating TCO is the cost of the product itself. For a traditional FISMA compliance approach, multiple product licenses are required for each product category (SIEM and log management, configuration auditing, network behavioral analysis, and file integrity monitoring). Using eIQnetworks’ SecureVue, only one product license is required; the ability to address all four functional areas – SIEM, configuration auditing, NBA, and FIM – is included out-of-box.

FISMA Security Compliance Solution Cost Category: Product License					
Category	Integrated Solution	Point Product Approach			
	SecureVue	All Are Required for FISMA Security Compliance			
		SIEM/LM	Config Audit	NBA	FIM
Product License	\$ 469,995	\$ 260,000	\$ 200,000	\$ 80,000	\$ 60,000
<b>TOTAL COST</b>	<b>\$ 469,995</b>	<b>\$ 600,000</b>			
Integrated Solution Cost Savings (\$)	\$ 130,005				
Integrated Solution Cost Savings (%)	21.67%				

Table 1: Product License Cost Comparison for FISMA Compliance Solutions

A traditional multiple-tool approach can lead to significant issues that can incur additional costs related to vendor management that are not calculated in this scenario, such as:

- **Disparate License Models.** Different license models require the organization to carefully estimate initial licenses to ensure that personnel, assets, and data are clearly quantified.
- **License Scalability.** Multiple license models also make scalability difficult. In many cases, adding personnel or assets to vendor solutions “resets” maintenance and other agreements, adding further complexity to the vendor management process.

***In this typical, conservatively-priced model, an integrated FISMA compliance approach will save the organization at least \$130,000 in initial product license costs, an almost 22% savings over a traditional multiple point security solution approach. This excludes additional cost savings in FTE personnel required to address potential vendor management issues identified above.***

## Annual Support and Maintenance Costs

For enterprise products such as FISMA compliance solutions, maintenance is a critical component to the solution lifecycle. In a traditional FISMA compliance approach, multiple maintenance agreements must be maintained for each product; on the other hand using an integrated solution such as eIQnetworks’ SecureVue, there is only a single maintenance license that needs to be purchased.

FISMA Security Compliance Solution Cost Category: Support and Maintenance (3 Years)					
Category	Integrated Solution SecureVue	Point Product Approach			
		All Are Required for FISMA Security Compliance			
		SIEM/LM	Config Audit	NBA	FIM
Support and Maintenance	\$ 281,997	\$ 156,000	\$ 120,000	\$ 48,000	\$ 32,000
<b>TOTAL COST</b>	<b>\$ 281,997</b>	<b>\$ 356,000</b>			
Integrated Solution Cost Savings (\$)	\$ 74,003				
Integrated Solution Cost Savings (%)	20.79%				

Table 2: Product Support and Maintenance Comparison for FISMA Compliance Solutions

Vendor management becomes a critical requirement using a traditional point solution approach, since significant issues can arise related to juggling multiple contracts, such as:

- **Multiple Termination Points.** With multiple maintenance agreements in place, organizations may run into inconsistent termination points for support, which can be exacerbated by scaling the vendors’ product to support additional users, assets, and/or data volumes.
- **Inconsistent Term and Condition Requirements.** Working with multiple vendors means having multiple sets of product use terms and conditions, which might include significant clauses related to product usability and scope, as well as different legal remedies.

***In the standard scenario presented in this paper, an integrated FISMA compliance approach will save the organization at least \$74,000 in aggregate support and maintenance costs over the initial three years of the solution. This represents an almost 21% savings over a traditional point solution-based approach, and excludes any additional costs associated with a traditional approach due to potential support and maintenance concerns identified above.***

## Training Costs

Training is critical to the operation security and compliance products. Inefficient use of security and compliance software can lead to ineffective implementation of security controls, and significant lapses in compliance reporting capability.

FISMA Security Compliance Solution Cost Category: Training						
Category	Integrated Solution	Point Product Approach				
	SecureVue	All Are Required for FISMA Security Compliance				
		SIEM/LM	Config Audit	NBA	FIM	
Training	\$ 15,000	\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000	
<b>TOTAL COST</b>	<b>\$ 15,000</b>	<b>\$ 40,000</b>				
<b>Integrated Solution Cost Savings (\$)</b>		<b>\$ 25,000</b>				
<b>Integrated Solution Cost Savings (%)</b>		<b>62.50%</b>				

Table 3: Product Training Comparison for FISMA Compliance Solutions

In a traditional FISMA compliance approach, additional “hidden” costs can be incurred due to potential issues such as:

- Inconsistent Training Quality.** With multiple vendors, initial product training quality and training consistency between vendors may vary greatly.
- Inconsistent Training Delivery Methods.** If a uniform training delivery method is not available – and specifically, a training method that is preferred by the customer – significant gaps in product operational knowledge may surface.
- Extended Time to Comprehensive Training.** Training personnel on multiple security point solutions will require multiple training periods, regardless of the delivery method of the training materials.

***In the standard scenario presented in this paper, an integrated FISMA compliance approach will save the organization at least \$25,000 over the initial three years of the solution, a 62.5% savings over a traditional point solution-based approach. This excludes additional costs related to potential training issues identified above.***

## Professional Services

“Professional services” is a broad cost category that may include: product deployment architecture; hands-on implementation; and product customization. Some products, such as most SIEM and log management tools, may also require significant software development time for the purpose of developing “connectors,” “adapters” and other interfacing components.

FISMA Security Compliance Solution Cost Category: Professional Services						
Category	Integrated Solution	Point Product Approach				
	SecureVue	All Are Required for FISMA Security Compliance				
		SIEM/LM	Config Audit	NBA	FIM	
Deployment Architecture and Design	\$ 2,500	\$ 5,000	\$ 5,000	\$ 2,500	\$ 2,500	
Implementation/Customization Services	\$ 10,000	\$ 62,500	\$ 62,500	\$ 10,000	\$ 10,000	
<b>TOTAL COST</b>	<b>\$ 12,500</b>	<b>\$ 160,000</b>				
<b>Integrated Solution Cost Savings (\$)</b>		<b>\$ 147,500</b>				
<b>Integrated Solution Cost Savings (%)</b>		<b>92.19%</b>				

Table 4: Professional Services Comparison for FISMA Compliance Solutions

In addition to the fact that multiple point tools will likely require multiple professional services engagements, there are additional concerns related to the cost of professional services for a multiple security tool approach:

- Project Management Integration Issues.** Enterprise software such as a FISMA compliance solution does not get implemented overnight; it requires the organization to carefully plan, communicate, and deploy the solution over time. However, for traditional solutions based on multiple security point tools, these project management concerns can become exacerbated by the need to deploy multiple servers, databases, and other infrastructure necessary to implement each point product.
- Software Development Requirements.** Many security point solutions – and SIEM and log management products, in particular – are built around “connector” and “adapter” components that provide customers with the flexibility to collect data from non-standard sources that require extensive subject matter expertise to ensure successful development. This can often result in vendor “lock-in” as the customer is forced to utilize the limited professional services of the vendor in order to derive real value from their product.

***In the standard scenario presented in this paper, an integrated FISMA compliance approach will save the organization at least \$147,500 in professional services over the initial three years of the solution, a significant 91% savings over a traditional point solution-based approach.***

## Operations Personnel

One of the most significant costs of ownership for information security and compliance software is the cost of personnel to operate and maintain the system. Operations personnel typically fall into two categories: product administrators who are responsible for all aspects of managing the product, and product database administrators who are responsible for maintaining the large databases that back-end most security and compliance products (usually relational database management systems).

FISMA Security Compliance Solution Cost Category: Operations Personnel					
Category	Integrated Solution	Point Product Approach			
	SecureVue	All Are Required for FISMA Security Compliance			
		SIEM/LM	Config Audit	NBA	FIM
Product Administrator (3 Years)	\$ 300,000	\$ 300,000	\$ 150,000	\$ 150,000	\$ 150,000
Database Administrator (3 Years)	\$ -	\$ 300,000	\$ 75,000	\$ 75,000	\$ 75,000
<b>TOTAL COST</b>	<b>\$ 300,000</b>	<b>\$ 1,275,000</b>			
Integrated Solution Cost Savings (\$)	\$ 975,000				
Integrated Solution Cost Savings (%)	76.47%				

Table 5: Operations Personnel Comparison for FISMA Compliance Solutions

Product administration costs are significantly lower for an integrated solution such as eIQnetworks’ SecureVue, due to the fact that SecureVue uses a proprietary, self-maintaining database that is designed for scalability and performance.

From an operations perspective, there are additional risks to a traditional point product approach that are not captured in the above table, including:

- Single Point of Failure for Product Knowledge.** In a traditional FISMA compliance solution approach involving multiple security products, each product typically has a limited number of users. This leaves a critical single point of failure for individual security products in the environment if a key employee with unique knowledge leaves the organization. The only alternative to mitigate this issue is to cross-train multiple employees on each solution – which adds significant cost to the overall solution.

**In the standard scenario presented in this paper, an integrated FISMA compliance approach – and specifically, a solution which has no DBA requirements, such as SecureVue – will save the organization at least \$975,000 in fully-loaded operations personnel costs over the initial three years of the solution, a 76% savings over the operational costs of a traditional point solution-based approach.**

## Conclusion

Based on the cost analysis and typical assumptions presented above, it is clear that a traditional FISMA compliance approach based on multiple point products – while perhaps effective at meeting rudimentary FISMA automation and compliance reporting – is a significantly more expensive approach than an integrated solution based on a single, enterprise product.

### Cost Comparison Table

Collectively, the following table presents the total cost of ownership comparison of list pricing between the traditional multi-product approach, versus an integrated solution such as eIQnetworks' SecureVue:

FISMA Security Compliance Solution Cost Category: Overall TCO						
Category	Integrated Solution SecureVue	Point Product Approach				
		All Are Required for FISMA Security Compliance				
		SIEM/LM	Config Audit	NBA	FIM	
Product License	\$ 469,995	\$ 260,000	\$ 200,000	\$ 80,000	\$ 60,000	
Support and Maintenance	\$ 281,997	\$ 156,000	\$ 120,000	\$ 48,000	\$ 32,000	
Training	\$ 15,000	\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000	
Deployment Architecture and Design	\$ 2,500	\$ 5,000	\$ 5,000	\$ 2,500	\$ 2,500	
Implementation/Customization Services	\$ 10,000	\$ 62,500	\$ 62,500	\$ 10,000	\$ 10,000	
Product Administrator (3 Years)	\$ 300,000	\$ 300,000	\$ 150,000	\$ 150,000	\$ 150,000	
Database Administrator (3 Years)	\$ -	\$ 300,000	\$ 75,000	\$ 75,000	\$ 75,000	
<b>TOTAL COST</b>	<b>\$ 1,079,492</b>	<b>\$ 2,431,000</b>				
Integrated Solution Cost Savings (\$)	\$ 1,351,508					
Integrated Solution Cost Savings (%)	55.59%					

Table 6: Overall TCO Comparison for FISMA Compliance Solutions

**Based on the typical scenario and relatively conservative assumptions presented in this paper, an integrated FISMA approach based on a unified threat and compliance solution – such as SecureVue from eIQnetworks – will save a typical organization at least \$1,350,000 in acquisition and operating costs over the initial three years of the solution, an almost 56% cost savings versus a traditional point solution-based approach over a three-year period.**

### Cost Comparison Charts

Visualizing this data as an aggregate across both approaches, the following chart demonstrates the clearly lower TCO provided by an integrated solution such as SecureVue as compared to a traditional point-product approach, both in terms of overall solution cost, as well as by individual cost category:

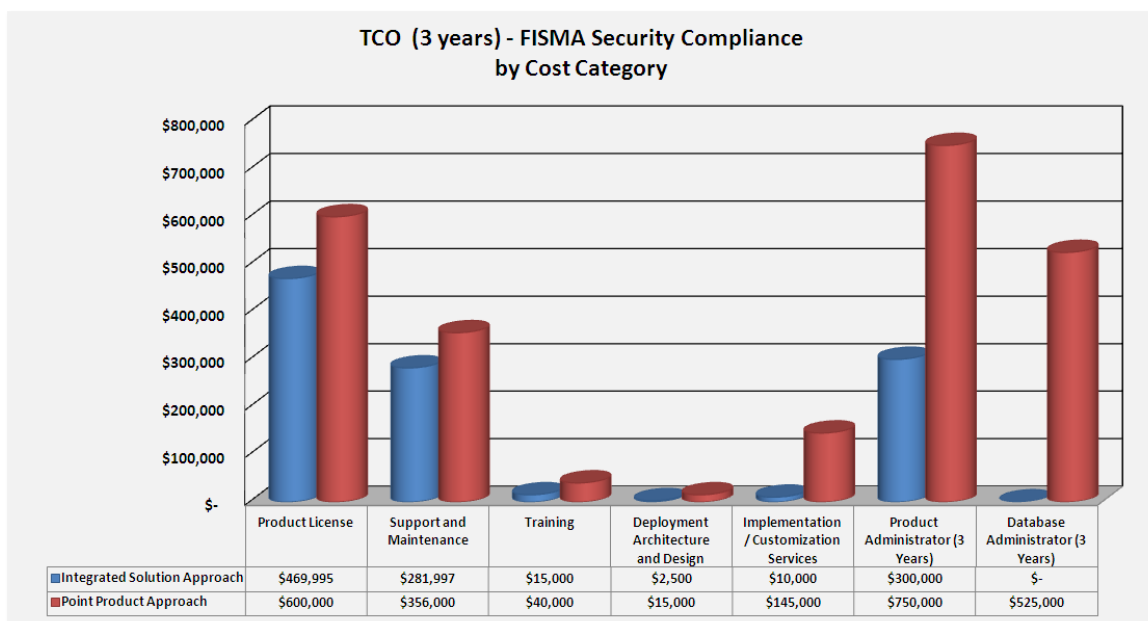
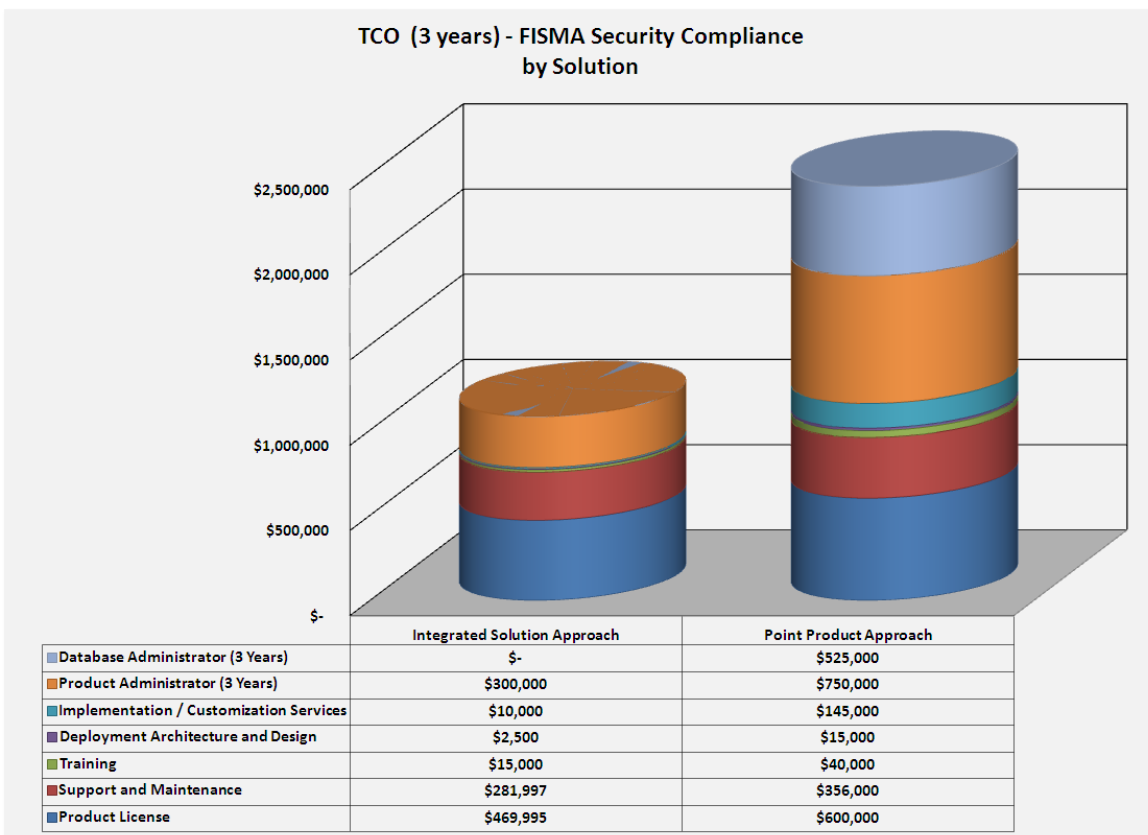


Figure 3: Three-Year FISMA Compliance TCO by Solution and Cost Category

Based on the TCO analysis presented in this paper, the following conclusions can be drawn:

- *A point solution approach to FISMA compliance, while it may be effective for FISMA automation and reporting, is highly cost-inefficient due to the need to replicate hardware, training, professional services, and other cost impacts across multiple products.*
- *An integrated solution that combines many aspects of FISMA compliance reporting and security operations yields a more cost-effective approach, while circumventing other issues that affect point solutions, such as scalability and the lack of situational awareness.*
- *Operational factors associated with an integrated solution provide additional value that goes beyond the cost calculations presented in this document: factors such as scalability, performance, faster return on investment, and other advantages of using an integrated solution will provide aggregate value above and beyond the “hard” costs presented here.*

## Appendix 'A': Detail of Security Data Type by NIST 800-53 Control Category

The following table provides a detailed overview of the specific types of information security data required to address individual controls with NIST 800-53 control categories:

Control Categories and Controls	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
<b>AC - Access Control</b>								
AC-1 - Access Control Policy and Procedures	-	-	-	-	-	-	■	-
AC-2 - Account Management	■	■	■	■	-	-	-	-
AC-3 - Access Enforcement	■	■	■	■	-	-	-	-
AC-4 - Information Flow Enforcement	■	■	■	■	-	-	-	-
AC-5 - Separation of Duties	-	-	-	-	-	-	■	-
AC-6 - Least Privilege	■	■	■	■	-	■	-	-
AC-7 - Unsuccessful Login Attempts	-	-	■	-	-	-	-	-
AC-8 - System Use Notification	-	■	-	-	-	-	-	-
AC-9 - Previous Login Notification	-	■	-	-	-	-	-	-
AC-10 - Concurrent Session Control	-	■	■	-	-	-	-	-
AC-11 - Session Lock	-	■	■	-	-	-	-	-
AC-12 - Session Termination	-	■	■	-	-	-	-	-
AC-13 - Supervision and Review - Access Control	-	-	-	-	-	-	■	-
AC-14 - Permitted Actions Without Identification or Authentication	-	-	■	■	-	-	■	-
AC-15 - Automated Marking	-	-	-	-	-	-	■	-
AC-16 - Automated Labeling	-	-	-	-	-	-	■	-
AC-17 - Remote Access	■	■	■	-	-	-	■	-
AC-18 - Wireless Access Restrictions	■	■	■	■	-	-	-	-
AC-19 - Access Control for Portable and Mobile Devices	■	■	■	■	-	-	-	-
AC-20 - Use of External Information Systems	■	■	■	■	-	-	-	-
<b>AT - Awareness and Training</b>								
AT-1 - Security Awareness and Training Policy and Procedures	-	-	-	-	-	-	■	-
AT-2 - Security Awareness	-	-	-	-	-	-	■	-
AT-3 - Security Training	-	-	-	-	-	-	■	-
AT-4 - Security Training Records	-	-	-	-	-	-	■	-
AT-5 - Contact with Security Groups and Associations	-	-	-	-	-	-	■	-

Control Categories and Controls	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
<b>AU - Audit and Accountability</b>								
AU-1 - Audit and Accountability Policy and Procedures	-	-	-	-	-	-	■	-
AU-2 - Auditable Events	■	■	■	■	■	■	-	■
AU-3 - Content of Audit Records	■	■	■	■	■	■	-	-
AU-4 - Audit Storage Capacity	■	■	-	-	-	-	-	-
AU-5 - Response to Audit Processing Failures	■	-	-	-	-	-	-	-
AU-6 - Audit Monitoring, Analysis and Reporting	■	■	■	-	-	-	-	-
AU-7 - Audit Reduction and Report Generation	-	-	-	-	-	-	■	-
AU-8 - Time Stamps	-	■	■	-	-	-	-	-
AU-9 - Protection of Audit Information	-	■	■	-	-	-	-	-
AU-10 - Non-Repudiation	■	■	■	-	-	-	-	-
AU-11 - Audit Record Retention	-	■	■	-	-	-	-	-
<b>CA - Certification, Accreditation, and Security Assessments</b>								
CA-1 - Certification, Accreditation, and Security Assessment Policies and Procedures	-	-	-	-	-	-	■	-
CA-2 - Security Assessments	■	■	■	■	■	■	■	■
CA-3 - Information Security Connections	■	■	-	■	-	-	-	-
CA-4 - Security Certification	■	■	■	■	■	■	■	■
CA-5 - Plan of Action and Milestones (POAM)	-	-	-	-	-	-	■	-
CA-6 - Security Accreditation	-	-	-	-	-	-	■	-
CA-7 - Continuous Monitoring	■	■	■	■	■	■	■	■
<b>CM - Configuration Management</b>								
CM-1 - Configuration Management Policy and Procedures	-	-	-	-	-	-	■	-
CM-2 - Baseline Configuration	■	■	-	-	-	■	-	-
CM-3 - Configuration Change Control	■	■	■	-	-	■	-	-
CM-4 - Monitoring Configuration Changes	■	■	-	-	-	■	-	-
CM-5 - Access Restrictions for Change	■	■	■	-	-	■	-	-
CM-6 - Configuration Settings	■	■	■	-	-	■	-	-
CM-7 - Least Functionality	■	■	■	-	-	■	-	-
CM-8 - Information System Component Inventory	■	-	-	-	-	-	-	-
<b>CP - Contingency Planning</b>								
CP-1 - Contingency Planning Policy and Procedures	-	-	-	-	-	-	■	-
CP-2 - Contingency Plan	-	-	-	-	-	-	■	-
CP-3 - Contingency Training	-	-	-	-	-	-	■	-
CP-4 - Contingency Plan Testing and Exercises	■	■	■	■	■	■	■	■

Control Categories and Controls	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
CP-5 - Contingency Plan Update	-	-	-	-	-	-	■	-
CP-6 - Alternate Storage Site	-	-	-	-	-	-	■	■
CP-7 - Alternate Processing Site	-	-	-	-	-	-	■	■
CP-8 - Telecommunications Services	-	-	-	-	-	-	■	■
CP-9 - Information System Backup	■	■	■	-	-	-	■	-
CP-10 - Information System Recovery and Reconstruction	■	■	■	■	■	■	■	■
<b>IA - Identification and Authentication</b>								
IA-1 - Identification and Authentication Policy and Procedures	-	-	-	-	-	-	■	-
IA-2 - User Identification and Authentication	■	■	■	■	-	-	-	-
IA-3 - Device Identification and Authentication	■	■	■	■	-	-	-	-
IA-4 - Identifier Management	■	■	■	-	-	-	■	■
IA-5 - Authenticator Management	■	■	■	-	-	-	■	■
IA-6 - Authenticator Feedback	■	■	■	-	-	-	-	■
IA-7 - Cryptographic Module Authentication	■	■	■	■	-	-	-	-
<b>IR - Incident Response</b>								
IR-1 - Incident Response Policy and Procedures	-	-	-	-	-	-	■	-
IR-2 - Incident Response Training	-	-	-	-	-	-	■	-
IR-3 - Incident Response Testing and Exercises	■	■	■	■	■	■	■	■
IR-4 - Incident Handling	■	■	■	■	■	■	■	■
IR-5 - Incident Monitoring	■	■	■	■	■	■	■	■
IR-6 - Incident Reporting	■	■	■	■	■	■	■	■
IR-7 - Incident Response Assistance	-	-	-	-	-	-	■	-
<b>MA - System Maintenance</b>								
MA-1 - System Maintenance Policy and Procedures	-	-	-	-	-	-	■	-
MA-2 - Controlled Maintenance	■	■	■	-	-	-	-	-
MA-3 - Maintenance Tools	■	■	■	-	-	-	-	-
MA-4 - Remote Maintenance	■	■	■	■	-	-	-	-
MA-5 - Maintenance Personnel	-	-	-	-	-	-	■	-
MA-6 - Timely Maintenance	-	-	-	-	-	-	■	-

Control Categories and Controls	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
<b>MP - Media Protection</b>								
MP-1 - Media Protection Policy and Procedures	-	-	-	-	-	-	■	-
MP-2 - Media Access	■	■	■	-	-	-	-	■
MP-3 - Media Labeling	-	-	-	-	-	-	■	-
MP-4 - Media Storage	-	-	-	-	-	-	■	■
MP-5 - Media Transport	-	-	-	-	-	-	■	■
MP-6 - Media Sanitization and Disposal	■	■	■	-	-	-	■	■
<b>PE - Physical and Environmental Protection</b>								
PE-1 - Physical and Environmental Protection Policy and Procedures	-	-	-	-	-	-	■	-
PE-2 - Physical Access Authorizations	-	-	-	-	-	-	■	■
PE-3 - Physical Access Control	-	-	■	-	-	-	■	■
PE-4 - Access Control for Transmission Medium	-	-	-	-	-	-	■	■
PE-5 - Access Control for Display Medium	-	-	-	-	-	-	■	■
PE-6 - Monitoring Physical Access	-	-	■	-	-	-	■	■
PE-7 - Visitor Control	-	-	■	-	-	-	■	■
PE-8 - Access Records	-	-	■	-	-	-	■	■
PE-9 - Power Equipment and Power Cabling	-	-	-	-	-	-	■	■
PE-10 - Emergency Shutoff	■	■	-	-	-	-	■	■
PE-11 - Emergency Power	-	-	-	-	-	-	■	■
PE-12 - Emergency Lighting	-	-	-	-	-	-	■	■
PE-13 - Fire Protection	-	-	-	-	-	-	■	■
PE-14 - Temperature and Humidity Controls	■	■	-	-	-	-	■	■
PE-15 - Water Damage Protection	-	-	-	-	-	-	■	■
PE-16 - Delivery and Removal	-	-	-	-	-	-	■	■
PE-17 - Alternate Work Site	-	-	-	-	-	-	■	■
PE-18 - Location of Information Security Components	-	-	-	-	-	-	■	■
PE-19 - Information Leakage	■	■	■	-	-	-	■	■
<b>PL - Planning</b>								
PL-1 - Security Planning Policy and Procedures	-	-	-	-	-	-	■	-
PL-2 - System Security Plan	-	-	-	-	-	-	■	-
PL-3 - System Security Plan Update	-	-	-	-	-	-	■	-
PL-4 - Rules of Behavior	-	-	-	-	-	-	■	-
PL-5 - Privacy Impact Assessment	-	-	-	-	-	-	■	-
PL-6 - Security-Related Activity Planning	-	-	-	-	-	-	■	-

Control Categories and Controls	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
<b>PS - Personnel Security</b>								
PS-1 - Personnel Security Policy and Procedures	-	-	-	-	-	-	■	-
PS-2 - Position Categorization	-	-	-	-	-	-	■	-
PS-3 - Personnel Screening	-	-	-	-	-	-	■	-
PS-4 - Personnel Termination	■	■	■	-	-	-	■	-
PS-5 - Personnel Transfer	■	■	■	-	-	-	■	-
PS-6 - Access Agreements	-	-	■	-	-	-	■	■
PS-7 - Third-Party Personnel Security	-	-	-	-	-	-	■	■
PS-8 - Personnel Sanctions	-	-	-	-	-	-	■	-
<b>RA - Risk Assessment</b>								
RA-1 - Risk Assessment Policy and Procedures	-	-	-	-	-	-	■	-
RA-2 - Security Categorization	-	-	-	-	-	-	■	-
RA-3 - Risk Assessment	■	■	■	■	■	■	■	■
RA-4 - Risk Assessment Update	-	-	-	-	-	-	■	-
RA-5 - Vulnerability Scanning	-	-	-	-	■	-	■	-
<b>SA - System and Services Acquisition</b>								
SA-1 - System and Services Acquisition Policy and Procedures	-	-	-	-	-	-	■	-
SA-2 - Allocation of Resources	-	-	-	-	-	-	■	-
SA-3 - Life Cycle Support	-	-	-	-	-	-	■	-
SA-4 - Acquisitions	-	-	-	-	-	-	■	-
SA-5 - Information Security Documentation	■	-	-	-	-	-	■	-
SA-6 - Software Usage Restrictions	■	■	■	-	-	-	■	-
SA-7 - User Installed Software	■	■	-	-	-	-	■	-
SA-8 - Security Engineering Principles	■	■	■	-	■	-	■	-
SA-9 - External Information System Services	-	-	-	-	-	-	■	-
SA-10 - Developer Configuration Management	■	■	■	-	-	-	■	-
SA-11 - Developer Security Testing	-	-	-	-	■	-	■	-
<b>SC - System and Communications Protection</b>								
SC-1 - System and Communications Protection Policy and Procedures	-	-	-	-	-	-	■	-
SC-2 - Application Partitioning	■	■	■	■	-	-	■	-
SC-3 - Security Function Isolation	-	-	-	-	-	-	■	-
SC-4 - Information Remnance	-	-	-	-	-	-	■	-
SC-5 - Denial of Service Protection	-	■	■	-	-	-	■	-

Control Categories and Controls	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
SC-6 - Resource Priority	-	-	-	-	-	-	■	-
SC-7 - Boundary Protection	■	■	■	■	-	-	-	-
SC-8 - Transmission Integrity	■	■	■	■	-	-	-	-
SC-9 - Transmission Confidentiality	■	■	■	■	-	-	-	-
SC-10 - Network Disconnect	-	■	■	-	-	-	-	-
SC-11 - Trusted Path	-	■	■	■	-	-	-	-
SC-12 - Cryptographic Key Establishment and Management	■	■	■	■	-	-	■	-
SC-13 - Use of Cryptography	■	■	■	■	-	-	■	-
SC-14 - Public Access Protections	■	■	■	■	-	-	-	-
SC-15 - Collaborative Computing	■	■	■	■	-	-	-	-
SC-16 - Transmission of Security Parameters	■	■	■	■	-	-	-	-
SC-17 - Public Key Infrastructure Certificates	■	■	■	■	-	-	-	-
SC-18 - Mobile Code	■	■	■	■	-	-	-	-
SC-19 - Voice Over Internet Protocol	■	■	■	■	-	-	-	-
SC-20 - Secure Name/Address Resolution Service (Authoritative Source)	■	■	■	■	-	-	-	-
SC-21 - Secure Name/Address Resolution Service (Recursive or Caching Resolver)	■	■	■	■	-	-	-	-
SC-22 - Architecture and Provisioning for Name/Address Resolution Service	■	■	■	■	-	-	-	-
SC-23 - Session Authenticity	■	■	■	■	-	-	-	-
<b>SI - System and Information Integrity</b>								
SI-1 - System and Information Integrity Policy and Procedures	-	-	-	-	-	-	■	-
SI-2 - Flaw Remediation	■	■	■	■	■	■	-	-
SI-3 - Malicious Code Protection	■	■	■	-	-	-	-	-
SI-4 - Information System Monitoring Tools and Techniques	■	■	■	■	■	■	■	-
SI-5 - Security Alerts and Advisories	-	-	-	-	■	-	■	-
SI-6 - Security Functionality Verification	■	■	■	■	■	■	■	■
SI-7 - Software and Information Integrity	■	■	■	■	-	■	■	-
SI-8 - Spam Protection	■	■	■	-	-	-	■	-
SI-9 - Information Input Restrictions	-	■	-	-	-	-	■	-
SI-10 - Information Accuracy, Completeness, Validity, and Authenticity	-	-	-	-	-	-	■	-
SI-11 - Error Handling	-	-	-	-	-	-	■	-
SI-12 - Information Output Handling and Retention	-	-	-	-	-	-	■	-