Meeting RMF Requirements around Compliance Monitoring

An EiQ Networks White Paper

Continuous Security Intelligence™

Meeting RMF Requirements around Compliance Monitoring

Continuous Security Intelligence™

Purpose

The purpose of this paper is to provide some background on the transition from DIACAP to the Risk Management Framework with an emphasis on the assessment process outlined in 800-53A.

What Happened to DIACAP?

On March 12, 2014, the Department of Defense officially adopted RMF as a replacement to DIACAP in DoD Instruction 8510.01.

As per 8510.01, all Department of Defense IS and PIT systems must "implement a corresponding set of security controls from NIST SP 800-53 (Reference (f)), and use assessment procedures from NIST SP 800-53A (Reference (g)) and DoD-specific assignment values, overlays, implementation guidance, and assessment procedures found on the Knowledge Service (KS)."

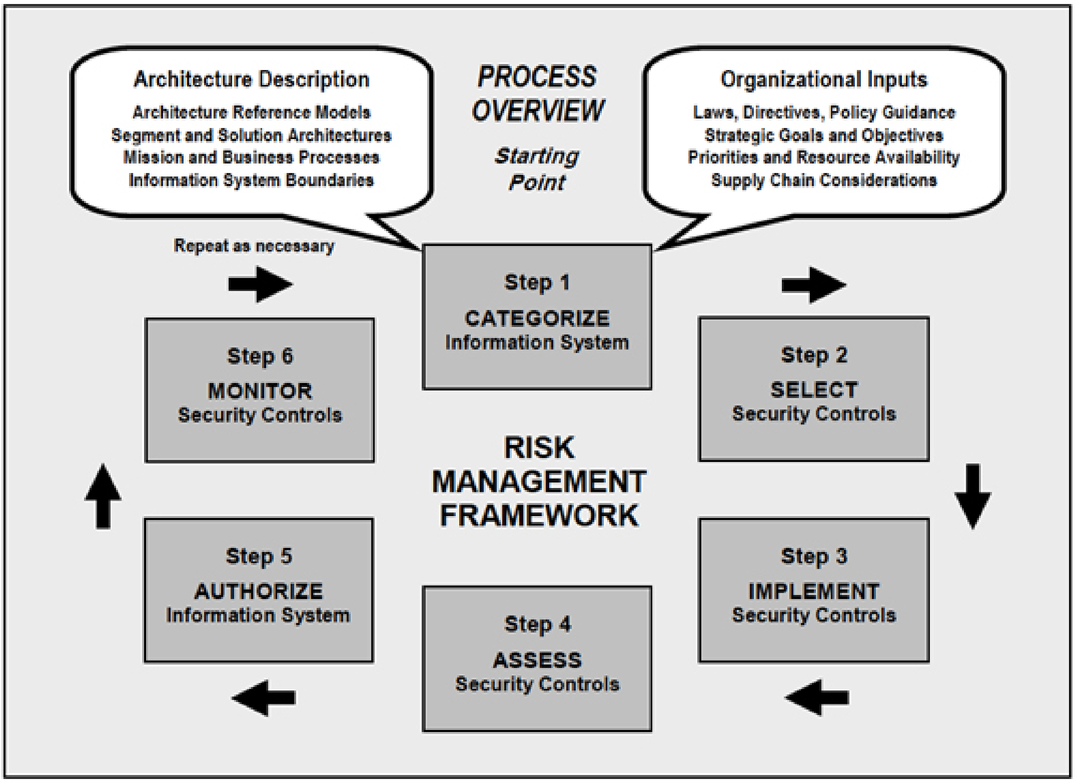
What is the Risk Management Framework (RMF)?

Details regarding Risk Management Framework (RMF) are spelled out in NIST Special Publication 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems." The Risk Management Framework is exactly that, a framework by which federal agencies can build their cyber security programs around. It is not about implementing a set of predefined controls. It's about implementing the RIGHT controls based upon the "mission and business objectives of the organization."

"The results of the security categorization process influence the selection of appropriate security controls for the information system and also, where applicable, the minimum assurance requirements for that system."

In other words, the controls selected are based upon the level of importance on the systems in question. Once the controls are selected and implemented, the next step is to assess the system to ensure it meets the cyber security controls selected in previous steps. Any weaknesses or gaps are documented and final authorization to allow the system to operate will be provided so long as the risks posed by gaps are deemed "acceptable." A key part of RMF is the last step that describes monitoring the security controls. In this step, organizations must:

- *Continuously monitor changes to the systems*
- *Analyze the "security impacts of identified changes"*
- *Conduct "ongoing assessments of security controls in accordance with the monitoring strategy"*
- *Remediate weaknesses on an ongoing basis*
- *Implement a process to report the security status to the authorizing official*
- *Update its critical risk management document routinely*
- *Conduct ongoing security authorizations*


Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Source: NIST SP 800-37

What is 800-53?

The NIST Special Publication 800-53 provides organizations with a set of security controls "necessary to fundamentally strengthen their information systems and the environments in which those systems operate" and guidance on what controls to implement, as not all systems are the same.

As stated through DODI 8510.01, all Department of Defense IS and PIT systems must “implement a corresponding set of security controls from NIST SP 800-53.” So in essence RMF is highly dependent upon what is outlined in 800-53.

Also contained within 800-53 is a list of controls that serve as a “starting point in determining the security controls for low-impact, moderate-impact, and high-impact information systems.” The controls are grouped into the following categories:

- *Access Control*
- *Awareness and Training*
- *Audit and Accountability*
- *Security Assessment and Authorization*
- *Configuration Management*
- *Contingency Planning*
- *Identification and Authentication*
- *Incident Response*
- *Maintenance*
- *Media Protection*
- *Physical Environmental Protection*
- *Planning*
- *Personnel Security*
- *Risk Assessment*
- *System and Services Acquisition*
- *System and Communications Protection*
- *System and Information Integrity*

What Does 800-53 Say about Configuration and Security Compliance Monitoring?

We have highlighted some sections below from 800-53 that are most applicable to the topic of configuration security and compliance monitoring. They are:

- *CA-7: Continuous Monitoring*
- *CM-3: Configuration Change Control*
- *CM-6: Configuration Settings*
- *CM-8: Information System Component Inventory*

Configuration Assessment (CA)

The CA series of controls within 800-53 deals with how security controls are assessed. Specifically it addresses the following:

- *Security assessments and authorization policy and procedures*
- *Security assessments*
- *System interconnections*
- *Security certification*
- *Plan of action and milestones*
- *Security authorization*
- *Continuous monitoring*
- *Penetration testing*
- *Internal system connections*

CA-7 Continuous Monitoring

In particular, CA-7 (Continuous Monitoring) states that organizations should develop and implement a continuous monitoring program that “facilitate[s] ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.” In essence, the organization should continuously measure whether the compliance against the 800-53 controls.

Moreover, such a program should provide “access to security-related information on a continuing basis through reports/ dashboards.” The organization should also perform trending analysis to “determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.”

Relevant Text from 800-53 regarding CA-7 Continuous Monitoring:

“The organization develops a continuous monitoring strategy and implements a continuous monitoring program”
“Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information.”

“The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.”

“Trend analyses can include, for example, examining recent threat information regarding the types of threat events that have occurred within the organization or across the federal government, success rates of certain types of cyber attacks, emerging vulnerabilities in information technologies, evolving social engineering techniques, results from multiple security control assessments, the effectiveness of configuration settings, and findings from Inspectors General or auditors.”

Configuration Management (CM)

The Configuration Management series of controls, CM, addresses concerns related to:

- *Establishment of a baseline configuration*
- *Configuration change control*
- *Security impact analysis*
- *Access restriction for change*
- *Configuration settings*
- *Least functionality*
- *Information system component inventory*
- *Configuration management plan*
- *Software usage restrictions*
- *User installed software*

CM-3 Configuration Change Control

Specifically CM-3 provides guidelines for how changes are introduced into environments in a controlled manner without inadvertently impact a system's security. Within CM-3, it outlines a series of automated mechanisms to accomplish this including the notification of authorities upon system configuration changes.

Relevant Text from 800-53 regarding CM-3 Continuous Monitoring:

"Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications."

The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify [authorities] of proposed changes to the information system and request change approval;

(c) Highlight proposed changes to the information system that have not been approved or disapproved by [defined time period];

(d) Prohibit changes to the information system until designated approvals are received;

(e) Document all changes to the information system; and

(f) Notify [defined personnel] when approved changes to the information system are completed.

CM-6 Configuration Settings

The "Configuration Settings", CM-6, control within 800-53 emphasizes the need to create a standard configuration setting for systems, implement the configuration settings, verify and approve any deviation from standard settings, and then monitor for changes to the settings.

CM-6 does not specifically state a standard baseline to use. Instead it references USGCB and SCAP as "common secure configurations". Within DoD, the common secure configuration are the DISA STIGs.

Relevant Text from 800-53 regarding CM-6 Configuration Settings:

"Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings."

"The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for information system components"

"The organization employs [security safeguards] to respond to unauthorized changes to [defined] configuration settings".

CM-8 Information System Component Inventory

The “Information System Component Inventory”, CM-8, control within 800-53 emphasizes the need to develop an “inventory of information system components” and develop automated mechanisms to detect unauthorized assets to include unauthorized software.

Relevant Text from 800-53 regarding CM-6 Configuration Settings:

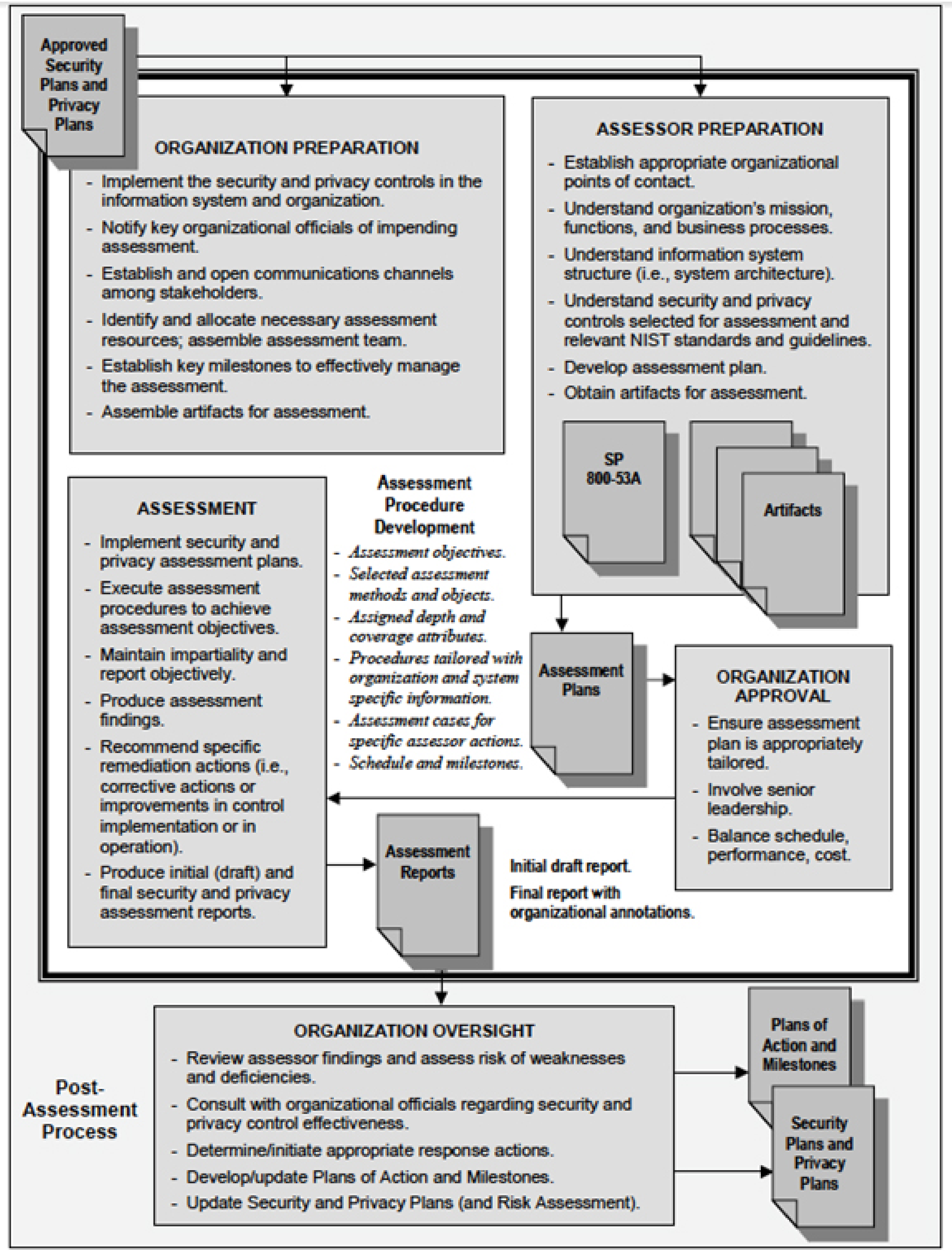
“The organization employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system;

“Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices.”

What is 800-53A?

Released December 2014, NIST Special Publication 800-53A Rev. 4 “provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations.” In other words, 800-53A provides more details on how to assess systems to determine whether the controls in 800-53 were correctly applied. The “findings produced by assessors are used to determine the overall effectiveness of security.”

The results of the assessment provide organizations with objective evidence whether the implemented controls are effective, insight into the quality of the risk management process, and “information about the strengths and weaknesses of information systems.”


Approved Security Plans and Privacy Plans
SP 800-53A
Artifacts
Assessment Plans
Assessment Reports
Plans of Action and Milestones
Security Plans and Privacy Plans
Post-Assessment Process

ORGANIZATION PREPARATION

- Implement the security and privacy controls in the information system and organization.
- Notify key organizational officials of impending assessment.
- Establish and open communications channels among stakeholders.
- Identify and allocate necessary assessment resources; assemble assessment team.
- Establish key milestones to effectively manage the assessment.
- Assemble artifacts for assessment.

ASSESSOR PREPARATION

- Establish appropriate organizational points of contact.
- Understand organization's mission, functions, and business processes.
- Understand information system structure (i.e., system architecture).
- Understand security and privacy controls selected for assessment and relevant NIST standards and guidelines.
- Develop assessment plan.
- Obtain artifacts for assessment.

ASSESSMENT

- Implement security and privacy assessment plans.
- Execute assessment procedures to achieve assessment objectives.
- Maintain impartiality and report objectively.
- Produce assessment findings.
- Recommend specific remediation actions (i.e., corrective actions or improvements in control implementation or in operation).
- Produce initial (draft) and final security and privacy assessment reports.

Assessment Procedure Development

- *Assessment objectives.*
- *Selected assessment methods and objects.*
- *Assigned depth and coverage attributes.*
- *Procedures tailored with organization and system specific information.*
- *Assessment cases for specific assessor actions.*
- *Schedule and milestones.*

ORGANIZATION APPROVAL

- Ensure assessment plan is appropriately tailored.
- Involve senior leadership.
- Balance schedule, performance, cost.

Initial draft report.

Final report with organizational annotations.

ORGANIZATION OVERSIGHT

- Review assessor findings and assess risk of weaknesses and deficiencies.
- Consult with organizational officials regarding security and privacy control effectiveness.
- Determine/initiate appropriate response actions.
- Develop/update Plans of Action and Milestones.
- Update Security and Privacy Plans (and Risk Assessment).

Source: NIST SP 800-37

Of particular importance, within Chapter 2.4, 800-53A outlines how organizations can make "the assessment process for security controls… more efficient and cost-effective" by leveraging Security Content Automation Protocol (SCAP). SCAP is one method that software tools can utilize to automatically assess the cyber posture of a system based upon misconfiguration, vulnerabilities, and patching. As a result, SCAP "enables organizations to identify and reduce vulnerabilities associated with products that are not patched or insecurely configured."

SCAP-validated tools can be used to automate the collection of assessment objects and evaluate these objects against expected behavior. The use of SCAP is specifically relevant to the testing of mechanisms that involve assessment of actual machine state. The National Checklist Program catalogs a number of SCAP-enabled checklists that are suitable for assessing the configuration posture of specific operating systems and applications.

> *”SCAP-validated tools can use these checklists to determine the aggregate compliance of a system against all of the configuration settings in the checklist (e.g., CM-6) or specific configurations that are relevant to a security or privacy control that pertains to one or more configuration settings. SCAP-validated tools can also determine the absence of a patch or the presence of a vulnerable condition. The results produced by the SCAP tools can then be examined by assessors as part of the security and privacy control assessments.”*

In essence, 800-53A encourages the use of tools that can automatically assess systems in a continuous manner against security controls.

How can SecureVue help with RMF Continuous Assessment?

SecureVue provides both the ability to assess systems against the 800-53 security controls as well as compliance against configuration standards such as the DISA STIGs on a number of network devices, servers, workstations, and applications. Such assessment capabilities are part of the overall SecureVue product suite which includes the functionality required for the 800-53 audit log management requirements

More specifically, SecureVue is a combined solution that meets critical information assurance/cyber security requirements for the Department of Defense

1. *Audit Log Management & SIEM*
2. *Continuous DISA STIG monitoring*
3. *Continuous Monitoring against the 800-53*

SecureVue’s Mapping to NIST SP 800-53

Requirement	Description	How SecureVue Addresses
AC-2	Automated Audit Actions	SecureVue can provide automated notifications to administrators upon the creation, modification, enabling, disabling, or removal of accounts.
AC-2	Account Monitoring/ Atypical	SecureVue reports atypical usage of information system accounts.
AC-3	Role-Based Access Control	SecureVue supports role-based access control to all features and data collected or utilized.
AC-7	Unsuccessful Logon Attempts	SecureVue can monitor and alert of unsuccessful logon attempts throughout the environment.

AC-10	Concurrent Session Control	SecureVue can be configured to limit the maximum number of users allowed as well as concurrent connections per user.
AU-2	Audit Events–Reviews and Updates	SecureVue allows administrators to easily audit events.
AU-3	Content of Audit Records	SecureVue will collect audit event data from a wide variety of networked devices. Data in audit events contains but not limited to: event type, time of event, location of event, source of event, outcome of event, and identify of individuals associated with event.
AU-4	Audit Storage Capacity	SecureVue has built in compression of 18:1 minimizing the amount of storage required to retain audit events.
AU-5	Response to Audit Processing Failures	SecureVue has built in administrative alerts that provide automated notifications in the event of an audit processing failure which include alerts when allocated audit record storage volume reaches organization-defined percentage of repository maximum audit record storage capacity.
AU-6	Audit Review Analysis and Reporting	SecureVue provides an automated way to conduct audit event review, analysis, and reporting.
AU-6	Correlate Audit Responses	SecureVue correlates audit event data across multiple data silos to help identify suspicious activity and provide greater situational awareness.
AU-6	Central Review and Analysis	SecureVue provides a central repository for the review of all audit event data across the enterprise.
AU-6	Integration/ Scanning and Monitoring Capabilities	SecureVue integrates with various enterprise capabilities such as vulnerability scanners for correlation against audit event data to further enhance the ability to identify inappropriate or unusual activity.
AU-7	Audit Reduction and Report Generation	SecureVue provides on-demand audit review through its web-enabled ForensicVue forensic search engine. This allows users to search through millions of events in seconds using an easy-to-navigate web interface. This capability eases after-the-fact investigations of security incidents. SecureVue also comes with hundreds of out-of-the-box alerts to meet all reporting requirements associated with this section.
AU-9	Protection of Audit Information	SecureVue protects audit events against unauthorized access, modification, and deletion by utilizing AES encryption in back-end data stores and ensuring that data cannot be accessed outside of SecureVue.
AU-11	Audit Record Retention	SecureVue can utilize local storage, network attached storage, or storage area networks. This enables SecureVue to meet all federal government audit retention requirements.

AU-12	Audit Generation	SecureVue can generate audit information from any data received by reports, alerts, or ad hoc searched.
CA-7	Continuous Monitoring	SecureVue continuously monitors systems against configuration standards as prescribed by DoD and DHS.
CA-9	Internal System Connections - Security Compliance Checks	SecureVue can be leveraged to ensure connecting systems are configured as prescribed by DISA STIGs or USGCBs.
CM-2	Baseline Configuration	SecureVue provides an automated mechanism for comparing information systems against custom baselines on industry standards such as DISA STIGs. SecureVue allows for administrators to easily see how systems deviate from baselines and retain previous baselines for comparison purposes.
CM-3	Configuration Change Control	SecureVue can be leveraged to validate proposed changes were successfully applied to systems. SecureVue can also be leveraged to notify administrators if changes were made to systems outside of the change window. SecureVue can also provide alerts to notify individuals if systems were changed outside of the prescribed baseline.
CM-6	Information System Component Inventory	SecureVue provide “an inventory of information system components” to include hardware, applications installed (version), services, users, shares, patches, vulnerabilities, etc. Using this inventory, SecureVue can then notify administrators of the presence of unauthorized software.
CM-11	User Installed Software	SecureVue “alerts organization-defined personnel or roles when the unauthorized installation of software is detected.”
IR-4	Incident Handling	SecureVue will assist in the detection of security incidents and automate creation of tickets based upon a series of detected events.
IR-5	Incident Monitoring	SecureVue provides a workflow to assist in tracking and documenting security incidents.
IR-6	Incident Reporting	SecureVue provides automated mechanisms to assist in the reporting of security incidents.
RA-5	Vulnerability Scanning – Review Historic Audit Logs	SecureVue can be leveraged to easily: • Determine if the organization reviews historic audit logs to see if a vulnerability identified in the information system has been previously exploited. • Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.
SI-4	Information System Monitoring	SecureVue can be configured to detect attack indicators and correlate information from various detection sources, providing a greater situational awareness picture.

Foundation of SecureVue

To better understand SecureVue's capabilities, it helps to understand how it works and its foundation. First, everything described in this paper can be accomplished without the need to deploy an endpoint agent. An agentless approach is important because it allows SecureVue to monitor systems for which agents can't be deployed such as network devices. SecureVue does have an optional agent, but deploying the agent is the exception, not the norm, and certainly not needed to realize all of the capabilities we are describing.

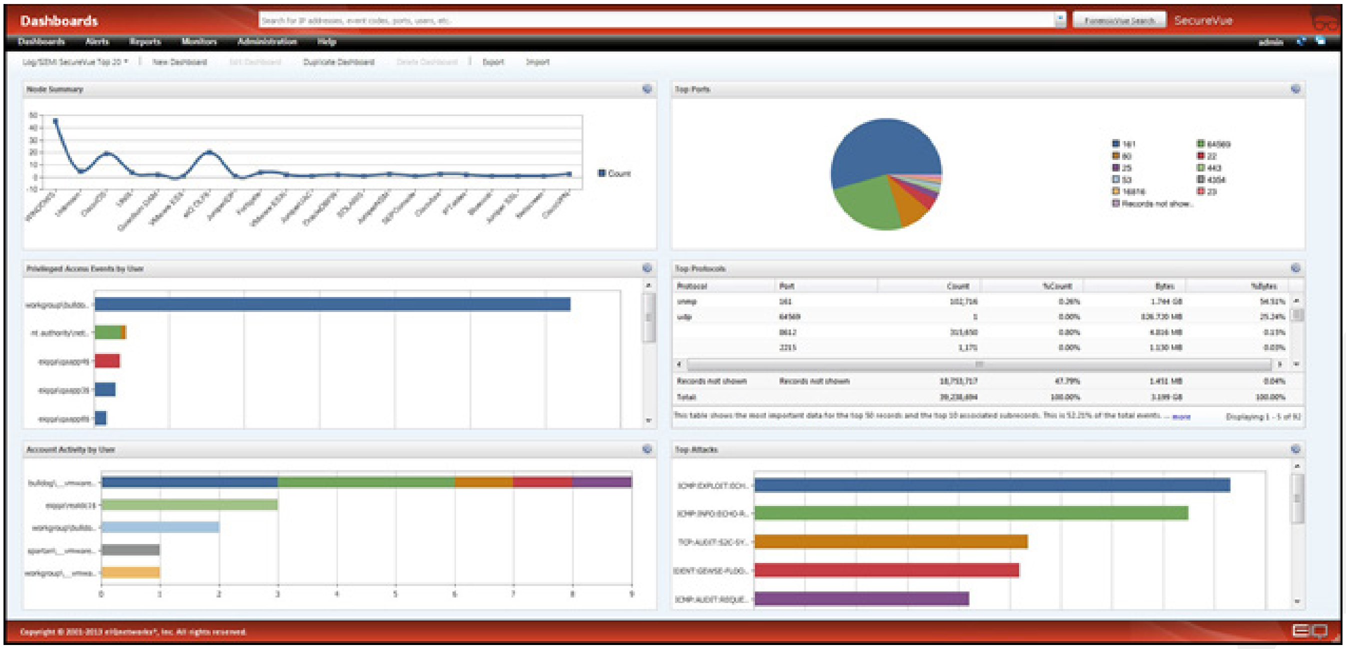
Without the agent, SecureVue will leverage protocols that exist in your network today. The protocol SecureVue will use to collect the data depends on A) the type of data being collected and B) the device it is collecting from. Naturally WMI won't work for your network devices while SSH won't work for your Windows systems. SecureVue will leverage both push and pull collections. In other words, some data SecureVue can collect passively such as syslog data or flow data. While other data requires an active pull. How SecureVue collects data and the protocols used are all done behind the scenes. You as an administrator only need to know what data you want to collect from which systems (or group of systems).

SecureVue will also leverage technology you have already deployed in your network to collect critical cyber security/information assurance data. These third party systems include you vulnerability scanners, anti virus solutions, and proxy/content filtering solutions, to name a few.

Now that you understand the foundation of SecureVue, explaining the full capabilities becomes a much easier task.

Continuous DISA STIG Monitoring

SecureVue's ability to monitor system state for asset and configuration changes makes it uniquely qualified to report compliance with industry configuration standards including DISA STIG, CIS, and USGCB.



Top Protocols

Protocol	Port	Count	%Count	Bytes	%Bytes
snmp	161	102,716	0.26%	1.744 GB	54.51%
udp	64569	1	0.00%	826.730 MB	25.34%
	8612	313,650	0.80%	4.816 MB	0.15%
	2215	1,171	0.00%	1.130 MB	0.03%
Records not shown	Records not shown	18,753,717	47.79%	1.451 MB	0.04%
Total		39,238,494	100.00%	3.199 GB	100.00%

This table shows the most important data for the top 50 records and the top 10 associated subrecords. This is 52.21% of the total events. ... more Displaying 1 - 5 of 6)

Key Benefits

Save Time with Automated Checks

SecureVue is saving organizations thousands of hours each year through automated checks.

Continuous View of Compliance vs. Point in Time

With SecureVue, users can now see compliance on a continuous basis. In the past, users relied on a point-and-shoot approach. In order to know compliance, they had to conduct a manual inspection of system.

Flexible Dashboards

SecureVue offers dozens of out of the box dashboards to display compliance data across the entire enterprise. New dashboards can be created in a matter of minutes through the simple point and click dashboard editor.

Extensive Reporting

Dozens of reports are available; all can be exported in various formats including PDF and CSV and can provide summary data such as overall level of compliance or compliance percentage over time. Detailed reports can provide the specifics about each control for each device checked (Host name, control name, control ID, severity, and status).

Compliance Alerts

SecureVue can be configured to notify selected individuals or groups regarding non-compliance, a change in compliance, or compliance that drops below a certain level. These alerts can be sent through an email, trouble ticket, or trap.

Custom Baselines

If you want to use SecureVue to track compliance against a custom baseline, no problem. With a few mouse-clicks, SecureVue can collect the configuration of a “gold-standard” device. That “gold standard” can be used to compare the compliance of all like devices.

SCAP and Beyond

SecureVue has received its FDCC and Authenticated Configuration SCAP validations. What’s important to note, however, is that SecureVue goes well beyond most SCAP-certified scanners, which are limited in they can only validate devices against compliance standards if there is SCAP content. If there is no SCAP content available, such as the case with the DISA STIGs for network devices and databases, SCAP dependent scanners will do nothing to automate the checks. To support the overall mission of automated and continuous compliance, EiQ has developed downloadable content for STIG checks and CIS policies when there is no SCAP content but demand exists for automated checks.

Exception Reporting

It is typically impossible for organizations to adhere 100% to any configuration standard. That is why SecureVue offers flexible exception tracking and reporting. For example, if you know there are certain controls which you will not be able to meet because it will break application or system, an exception can be created within SecureVue for that control. That exception can be applied to a single system, multiple systems, or a group of systems. Compliance results will take this exception in to account. In addition, a report can be easily generated to list all of the exceptions, the exception expiration date, and to what devices that exception applies.

SecureVue for Auditors

In those situations where auditors need tools to help automate compliance checks, SecureVue is available as an auditor's license.

Audit Log Management & SIEM

SecureVue® Log Management & SIEM provides industry-leading event and log collection, storage, correlation, reporting, and search functions for meeting all DoDI 8500.2 and NIST 800-53 Audit Log Management requirements. The solution supports a broad range of event sources including network infrastructure, security solutions, operating systems, and applications.

Automated Event Review

One of the key requirements pertaining to audit log management contained within NIST 800-53 and DoDI 8500.2 is the need to "review" events for suspicious activity. The challenge with this requirement is simply how does one go through the thousands of events that are generated daily to identify the ones that are "suspicious" or worthy of further inspection? This is one of the areas where SecureVue shines. Once SecureVue is collecting event data, it can automatically correlate and filter events and notify individuals which ones, if any, are considered suspicious or require further investigation. This automated method removes the need to manually review events and saves a tremendous amount of time.

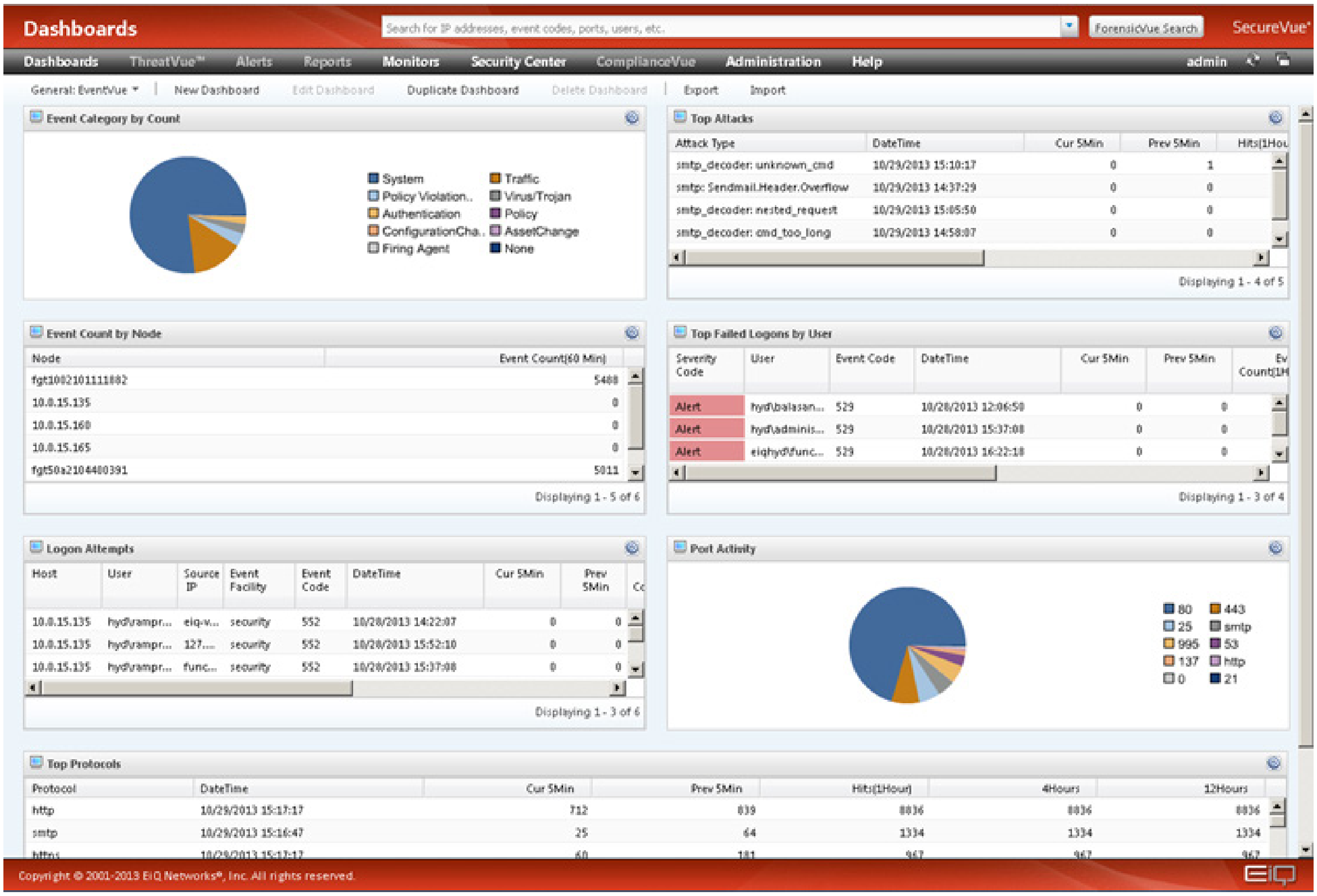
SecureVue comes with 600+ alerts and many that are tailored specifically to DoD and federal agencies. These alerts can be easily tailored via a GUI to meet any specific requirements you may have. Out-of-the-box alerts include notifications when the following events occur:

- *10 failed login attempts on a device from a single IP within a five-minute period*
- *Traffic that violates ports and protocols policies*
- *System are connected to network with missing required software (such as Host-Based IPS, Anti Virus) or systems with banned software (peer-to-peer)*
- *DNS queries from organization that query non-organization DNS servers*
- *Large data transfers to the Internet*
- *Long outbound connections*
- *Inbound traffic to Web servers not using TCP 80/443*
- *Multiple denies at the firewall followed by an allow (Single source IP address)*
- *SQL anomalies: the xp_cmdshell being enabled followed by user accounts added to local systems*
- *CPU Usage, Memory Usage, and low disk space*
- *Profiling service accounts*
- *Accounts added to local groups on servers*

Flexible Dashboard

SecureVue comes with 50+ dashboards out of the box that allow users to easily visualize the risk and operational picture of the network. Any dashboard can be easily tailored to meet specific requirements or user preferences, saved, and shared with others.

Dashboards can incorporate controls for both event and state data sets and are interactive so users can drill-down on them to get into greater details.



Top Attacks

Attack Type	DateTime	Cur 5Min	Prev 5Min	Hits(1Hou
smtp_decoder: unknown_cmd	10/29/2013 15:10:17	0	1	
smtp: Sendmail.Header.Overflow	10/29/2013 14:37:29	0	0	
smtp_decoder: nested_request	10/29/2013 15:05:50	0	0	
smtp_decoder: cmd_too_long	10/29/2013 14:58:07	0	0	

Displaying 1 - 4 of 5

Event Count by Node

Node	Event Count(60 Min)
fgt1002101111882	5488
10.0.15.135	0
10.0.15.160	0
10.0.15.165	0
fgt50a2104400391	5011

Displaying 1 - 5 of 6

Top Failed Logons by User

Severity Code	User	Event Code	DateTime	Cur 5Min	Prev 5Min	Ev Count(1H
Alert	hyd\balasan...	529	10/28/2013 12:06:50	0	0	
Alert	hyd\adminis...	529	10/28/2013 15:37:08	0	0	
Alert	eiqhyd\func...	529	10/28/2013 16:22:18	0	0	

Displaying 1 - 3 of 4

Logon Attempts

Host	User	Source IP	Event Facility	Event Code	DateTime	Cur 5Min	Prev 5Min	Co
10.0.15.135	hyd\rampr...	eiq-v...	security	552	10/28/2013 14:22:07	0	0	
10.0.15.135	hyd\rampr...	127....	security	552	10/28/2013 15:52:10	0	0	
10.0.15.135	hyd\rampr...	func...	security	552	10/28/2013 15:37:08	0	0	

Displaying 1 - 3 of 6

Port Activity

Top Protocols

Protocol	DateTime	Cur 5Min	Prev 5Min	Hits(1Hour)	4Hours	12Hours
http	10/29/2013 15:17:17	712	839	8836	8836	8836
smtp	10/29/2013 15:16:47	25	64	1334	1334	1334
https	10/29/2013 15:17:17	60	181	967	967	967

Copyright © 2001-2013 EiQ Networks®, Inc. All rights reserved.

Forensic Searching

Utilize ForensicVue®, an integrated component of SecureVue, to significantly decrease the time required to discover and visualize the root cause of security incidents. Organizations can use ForensicVue is almost the same manner as a search engine: getting answers to specific questions. For example, using ForensicVue you can quickly see all login events between 12:10 and 12:15 AM.

The results could be easily narrowed to search within those results for those login attempts using the user ID administrator.

What makes SecureVue even more powerful is the fact that searches can be conducted to go beyond event data and search within device state data. For example, you may want to run a search to show what systems are missing a particular patch or which systems have “Wireshark” installed.

Easy Setup and Management

The fact that SecureVue does not require an agent makes the setup and ongoing management much easier. SecureVue can begin monitoring hundreds of devices in hours. What also makes SecureVue much easier to manage is the fact that it does not utilize a relational database management system. This is important because many log management and SIEM systems require a RDBMS, which requires system administrators who know and understand these complex databases. With such systems, one needs to understand how to increase tablespace sizes, run import and export commands, create new indexes, and optimize the database. These are all DBA activities that may require training and certification in Oracle, MSSQL, or Sybase. With SecureVue, the database is a highly efficient, flat-file system, which means if you know how to use Windows Explorer you know how to manage the SecureVue database.

Configuration Monitoring Capability Description

Information Assurance requirements outlined in 800-53, 8500.2, and AR 25-2 require agencies and military installations to implement a broad set of people, processes and technologies to help protect government networks. Historically, the technology requirements meant the implementation of several point tools to meet the various requirements. SecureVue collects a broad array of data elements and as a result, can meet several of the IA requirements without the need to acquire multiple tools. SecureVue can meet requirements related to compliance management, configuration auditing, and audit log management within a single tool.