Continuous Monitoring in RMF

Continuous Monitoring in a Risk Management Framework consists of continuous assessments, reporting, and authorization of information systems to monitor security risks.

We employ several methods both automated and manual processes to protect the Information System as cost effectively as possible. Logical security controls that monitor access, and logs network traffic, unauthorized attempts to upload or change information, to cause damage, or to deny service to authorized users.

-Continuous Assessment

\*Automated

Tenable Nessus

Applicable Best Practices, STIGS, Benchmarks & SNAC guides

Nagios Monitoring - Real Time Monitoring

\*Manual

Audit and system log review

Best Practices, STIGS, Benchmarks & SNAC when they cannot be automated

-Continuous Reporting

\*Automated via Tenable Nessus

\*Manual review of Audit & Systems Logs of Servers, Network devices and AWS console

-Continous Authorization

\*System doesn’t currently pose a risk (No PII or sensitive data processed) and at any point can be turned off via sysadmins via AWS or system console.

\*Backend systems are only accessible via approved TWS sysadmins.

Tenable Nessus:

The Tenable Nessus continuous scanning is implemented on a virtual server that only scanning administrators can access.

Each “system of systems” has its own scanning profile that can be individually scheduled to implement Continuous Monitoring. The STIGs and other scanning profiles run against each server are custom-tailored to the target, and the scanning profiles automatically update from the vendor.

While the Nessus server is located in the AIS data center, it can scan any servers located on Amazon Web Services via VPN and/or configuring the target data center’s firewall to allow entry based on source and target IP, ensuring that Nessus can scan the targets securely while not increasing the attack surface of the target.

The Tenable Nessus solution is part of our automated compliance tool and will address the following:

|  |  |
| --- | --- |
| Multiple Assessment Types | |
| **Vulnerability scanning** | Assess systems, networks and applications for weaknesses |
| **Configuration auditing** | Ensure that IT assets are compliant with policy and standards |
| **Compliance checks** | Audit system configurations and content against standards |
| **Malware detection** | Detect malware as well as potentially unwanted and unmanaged software |
| **Web application scanning** | Discover web server and services weaknesses and OWASP vulnerabilities |
| **Sensitive data searches** | Identify private information on systems or in documents |
| **Control system auditing** | Scan SCADA systems, embedded devices and ICS applications |
| Ongoing Management | |
| **Product updates** | Nessus software and UI changes can be configured for automatic feeds |
| **Content updates** | Advanced threats, zero-day vulnerabilities and new types of regulatory compliance configurations |
| Connect with Core Systems | |
| **Nessus RESTful API** | Standard, supported and documented API for integrating Nessus into your workflow |
| Reporting | |
| **Flexible reporting** | Customize reports to sort by vulnerability or host, create an executive summary, or compare scan results to highlight changes |
| **Multiple report formats** | Native (XML), PDF (requires Oracle Java be installed on Nessus server), CSV, and HTML |
| **Targeted email notifications** | Notification of scan results, remediation recommendations and scan configuration improvements |

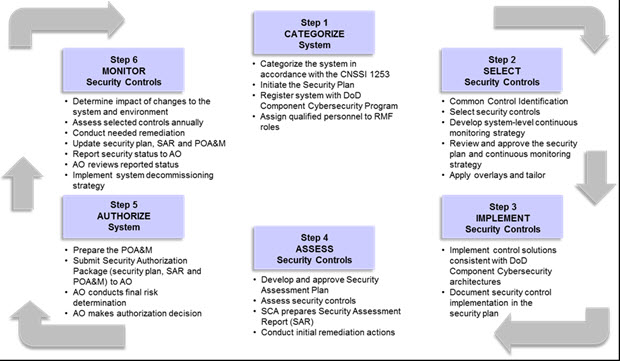
**Table 1: Nessus Features**

Systems logs from the servers, AWS environment and will be manually reviewed for suspicious patterns and activity as additional component of our CM.

## Nagios Core Overview

* **Comprehensive Monitoring:** Provides monitoring of all mission-critical infrastructure components - including applications, services, operating systems, network protocols, system metrics, and network infrastructure.
* **Visibility:** Provides central view of your entire IT operations network and business processes.
* **Awareness:** Alerts are delivered to IT staff via email and SMS. Multi-user notification escalation capabilities ensure alerts reach the attention of the right people.
* **Problem Remediation:** Event handlers allow you to automatically restart failed applications, services, servers, and devices when problems are detected.
* **Reports:** Ensure SLAs are being met, provides historical records of outages, notifications, and alert response for later analysis.
* **Extendable Architecture:** Provides easy integration with in-house and third-party applications. Hundreds of community-developed addons extend core functionality.

The system will require categorization per ref. A&B



**RMF for Information Systems**

The initial categorization of this system is:

Confidentiality = Low

Integrity = Low

Availability = Low

For an overall system categorization of “Low”.

Ref: **A Guide for Mapping Types of Information and Information Systems to Security Categories Vol1**

<http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf>

Ref: B **Guide for Mapping Types of Information and Information Systems to Security Categories Vol2**

<http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf>

Ref: C **Information Security Continuous Monitoring for Federal Information Systems and Organizations**

<http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>

Ref: D **Nessus Features**

<http://www.tenable.com/products/nessus/features#reporting>