University of South Florida

Cybersecurity Vulnerability Management: A Navy Program Assessment

A Comparative Analysis of Current Practices against Department of Defense, Navy, and Industry Standards for Vulnerability Identification, Remediation, and Mitigation

Nathan Rickett

ISM 6940

07 March 2025

Dr. Varol Kayhan

Table of Contents

Introduction

Problem Statement

The organization has a well-documented process for vulnerability management of customer systems but needed a centralized method to identify, analyze, report, remediate, and monitor vulnerabilities of internally owned assets. To resolve this issue, a small team was created and tasked with starting a vulnerability management program specifically for internal assets. The team understands the general requirements and common taskings associated with managing vulnerabilities specific to the Department of the Navy but lacks insight into whether the program could be operating more efficiently, and whether every requirement is being met. This poses a security risk to both the organization and customers. The desired outcome of this programmatic review is for the organization to be able to easily interpret the findings and implement recommendations where deemed necessary.

Purpose and Scope

The purpose of this research project is to assess the effectiveness of the organization's internal vulnerability management program, which will be beneficial to both the organization and to the author. By conducting this assessment, the author can demonstrate his ability to critically address issues relevant to cybersecurity, gain practical experience in cybersecurity management, and expand his understanding of the DoD vulnerability management process. The organization will benefit from having a greater insight into the effectiveness of the internal vulnerability management program, having a detailed list of recommendations for improvement, and increased awareness of risk and threats posed by internal vulnerabilities. The scope of this project includes an analysis of the current program, identification of rules and best practices, and recommendations for improvement.

Objectives

1) Analyze the current state of the vulnerability management program based on strategy development, plan creation, implementation, and continuous improvement.
2) Compare the analysis of the vulnerability management program state to rules, regulations, and industry standards.
3) Develop recommendations for enhancing the vulnerability management program to meet identified rules, regulations, and industry standards.

Research questions

1) How well does the program adhere to DoD mandates and guidelines?
2) How well does the program adhere to industry best practices?
3) How well is the organization assessing the effectiveness of the internal vulnerability management program?

Expected Outcomes

1) A comprehensive assessment of the organization's internal vulnerability management program is conducted, documented, and documentation is easily discernable.
2) The assessment documentation includes specific requirements based on rules, regulations, and best practices and whether the organization is meeting those requirements.
3) Each requirement that isn't met includes a recommendation for how to meet the requirement.
4) Implementation of recommendations will improve how efficiently and effectively the vulnerability management program approaches each step of the vulnerability management lifecycle.

Structure

This report is divided into several sections, each of which correlates with a step within the *CRR Resource Guide Volume 4: Vulnerability Management Version 1.1* document. The CRR Supplemental Resource Guide was funded and supported by the Department of Homeland Security under contract with Carnegie Mellon University and outlines each step necessary to creating, implementing, and assessing a vulnerability management program. The requirements listed in each table were developed by the author of this report and were derived from a culmination of requirements, best practices documents for vulnerability management, and personal experience working in the cybersecurity industry. These documents can be found in the references section of this report.

To ensure that the report stays in an easily discernable format, the following structure is implemented. Each guideline or requirement is posted within a table accompanied by a compliance score symbol underneath it. Compliance score symbols serve to quickly assess how well the organization is adhering to the section of the report. Each table is labeled with a category, and underneath it includes a definition, score explanation, and solution. The definition explains the meaning and importance of the category, while the score explanation provides a more in-depth explanation of how well the organization is complying with the requirement. Finally, a solution will be provided if the organization does not meet all the requirements in the table.

- Example Table

Requirement 1	Requirement 2	Requirement 3
✓	⊘	⊗

Definition:

Score Explanation:

Solution:

Compliance Score Symbols

- ✓ – The organization is fully compliant with every aspect of the requirement.
- ⊘ – The organization is partially compliant. Some aspects of the requirement may be implemented while others are not, or the requirement is implemented but not up to standard.
- ⊗ – No part of the requirement has been implemented.

Strategy Development

Defining a strategy ensures that the vulnerability management process stays aligned with the goals of the organization throughout its lifecycle. This step of the analysis seeks to understand whether organizational goals have been identified and if the organization has developed and documented a strategy for achieving those goals.

Determining the Scope

Statement of Purpose

A purpose statement has been documented	The purpose statement incorporates program objectives and provides a clear direction
⊗	⊗

Definition: A purpose statement provides directions for the organization and should be used as a reference throughout the vulnerability management program's lifecycle. All objectives of the program should be clearly identified in the purpose statement.

Score Explanation: A purpose statement has not been documented.

Solution: The following is a proposed statement of purpose:

"While the organization currently offers services for vulnerability identification and remediation, it is the responsibility of mission owners to track, assess, and manage those vulnerabilities belonging to their systems. Unlike mission owner systems, internally owned systems require that employees manage vulnerabilities at each phase of the vulnerability management process. Previously, this management process was delegated to each of the areas of responsibility (AORs) within the data center, which resulted in inconsistencies and low visibility of vulnerability coverage. The goal of an internal vulnerability management program is to make the vulnerability management a centralized effort, resulting in comprehensive visibility, standardization, improved compliance and reporting, and an overall strengthened security posture."

Asset Identification

Candidate assets and services have been identified	Candidate assets have been documented	Criticality ratings have been developed and assigned to assets
✓	✓	✓

Definition: Assets are a part of an organization's resources, and resources need to be identified prior to developing a plan. Resource constraints will often have a large impact on assessment and monitoring capabilities. Rating assets based on criticality helps the organization to prioritize which assets to focus protection efforts on first.

Score Explanation: Each system is required to have an "authority to operate" according to *OPNAVINST 5239.1E*. To adhere to this rule, the organization maintains a database of assets along with a

categorization. The organization's internal *Cyber Security Policy* document section 6.1 addresses how the systems are categorized.

Operational Environment Identification

Operational environments have been identified	Operational environments have been documented	Environments have been defined by exposures to threats of greatest concern
✓	✓	✓

Definition: The operational context determines the nature of threats and vulnerabilities that assets are subjected to. The organization should identify, categorize, and document all operational environments so that they can prioritize and allocate resources based on risk.

Score Explanation: The organization's internal *Cyber Security Policy* document defines each of the asset environments in section 1.2. Environments have also been prioritized in a separate document.

Selecting Management Methods

Candidate methods for vulnerability management

Candidate methods for vulnerability management have been identified	Candidate methods of vulnerability management have been documented	Candidate methods include all organization specific requirements and industry best practices	All candidate methods identified have an impact analysis	Methods of vulnerability management have been chosen
⃠	⊗	✓	⊗	✓

Definition: Not all methods of managing vulnerabilities will align with organizational risk appetite, organizational budget, or be accepted by every stakeholder. Therefore, all methods must first be identified, then narrowed down based on organizational needs. *DOD 8531.01* and *NIST Special Publication 800-137* contain key guidance on selecting vulnerability management methods.

Score Explanation: The internal vulnerability management program already deploys some methods of identifying, categorizing, tracking, and mitigating vulnerabilities, but no strategy documentation exists on why these methods were chosen, if there were other candidate methods that were identified prior to making the selection, and why the chosen methods were selected.

Solution: All candidate methods should be documented, including their financial and operational impacts. Chosen methods should have an explanation. According to *DOD 8531.01,* the following methods for vulnerability management are suggested:

Identification:

- Vulnerability scanning, Penetration Testing, Security Controls Assessment, Historical Documentation, Coordinated VDP, VEP.

Analysis**:**

- Impact Assessment, Analysis Prioritization.

Reporting**:**

- A Detailed analysis report including the name, date of discovery, correction recommendations, CVSS score and severity, details concerning loss of CIA.

Remediation and Mitigation:

- Ensure AORs have the appropriate information and allocation of resources to remediate or mitigate vulnerabilities in a timely manner.

Continuous Monitoring and Improvement**:**

- Continuously verify remediation or mitigation of vulnerabilities according to standards outlined in *DOD 8531.01* and *NIST Special Publication 800-137* and ensure that the program is updated in accordance with security status metrics.

Resourcing Activities

Stakeholders

Stakeholder roles have been identified	Stakeholder responsibilities have been identified	Stakeholder documentation exists	Stakeholders have been engaged
✓	✓	✓	✓

Definition: To ensure that the chosen methods of vulnerability management are capable of operating, all relevant parties need to be informed and engaged. Clearly identifying and documenting each role and their responsibilities prevents confusion and overlap.

Score Explanation: All relevant stakeholders have been identified and documented. Each stakeholder has been engaged and is aware of their role in vulnerability management.

Budget

A draft budget was created	Draft budget has been documented
⊗	⊗

Definition: Creating a draft budget will help to identify any gaps in the chosen methods of vulnerability management and may cause management to reconsider how the VMP should operate.

Score Explanation: No draft budget was identified.

Solution: If the organization has not already created a draft budget for the internal vulnerability management program, one should be created and documented to ensure that it is affordable.

Plan Creation

Strategy is nothing without a plan. Here the more granular implementation details are identified based on what was outlined in the strategy. The strategy is the organization's guiding principles, while the plan document is the roadmap containing specific instructions. The needs of one environment may be different from another, so it's important to iron out the technical details before trying to begin the management process. For example, identifying vulnerabilities in a Windows Operating System has different technical needs than identifying vulnerabilities in a facility perimeter.

Processes & Activities

Processes

The plan document provides a high-level overview of each vulnerability management process.	The purpose and scope of each process is clearly defined.	There is a logical flow or sequence between each process.	Processes required by rules, regulations, and best practices have been included.
⊗	⊗	⊗	⊘

Definition: A vulnerability management process is a broad overarching method for implementing the VMP. Processes can encompass all steps of the vulnerability management life cycle. Some examples include identification and vulnerability remediation.

Score Explanation: The plan document in its current form outlines some of the weekly activities and responsibilities of key stakeholders but does not have a section that describes each process involved with the vulnerability management program, nor its purpose and scope. The vulnerability management team is, however, aware of the main processes involved with implementing a vulnerability management program and their associated activities, since they are actively performing them daily. It is advised that a section be formally included in the plan document that describes each of the VMP processes along with their purpose and scope.

Solution: *DoDI 8531.01* provides a high-level overview for selecting vulnerability management processes, as well as their purpose and scope. Those processes in sequential order are:

1) Identification – Identification is one of the first steps involved with managing vulnerabilities and is a crucial step in the patch management lifecycle. The VMP team members will utilize manual efforts and automated security tools to detect potential vulnerabilities in the organization's assets.
2) Vulnerability Analysis – Assessing vulnerabilities is necessary for establishing a priority. The VMP team members will assess vulnerabilities by evaluating their impact and prioritizing them. This allows one to assign severity levels in a timely manner.
3) Analysis Reporting – Reporting the findings from the vulnerability analysis to relevant stakeholders is required for the remediation / mitigation of the vulnerability and could also be required by law or regulations depending on the nature of the work. The VMP team will create

reports in accordance with section 4.2.2 of *Risk Management Framework Risk Assessment Guide Version 2.0.*

4) Remediation / Mitigation - Remediation involves eliminating or removing the vulnerability. Mitigation involves reducing the impact of vulnerability without necessarily eliminating it. To properly remediate or mitigate vulnerabilities, VMP team members will implement all 11 steps outlined in *DoDI 8531.01* page 19.
5) Verification and Monitoring - Validate the effectiveness of the remediation or mitigation methods applied to identified vulnerabilities and conduct ongoing monitoring to prevent further exploitation

Some other processes not listed as a requirement but should still be considered are training & awareness, and escalation procedures.

Activities

Tasks/activities associated with each process have been defined	Dependencies of each activity have been identified	Each task/activity identified has a periodic time requirement
✓	⃠	✓

Definition: Each process in a VMP has associated tasks and activities which are necessary for implementing the processes. The plan document needs to include a general guideline for how each task is performed, how often it needs to be performed, and the dependencies needed for each activity.

Score Explanation: Tasks and activities have been outlined in the organization's plan document, but they aren't associated with a specific vulnerability management process. Including the process that an activity is associated with is a great way to structure a plan document. The organization is aware of required dependencies, but they are not explicitly stated in the plan document.

Solution: Identify and document activities involved with each process of vulnerability management. Also include how often the task should be performed and what the dependencies are. *DoD 8531.01 and RMF Risk Assessment Guide Version 2.0* are great sources for defining activities. Below are a few sample activities, each of which are associated with a process mentioned in the table above.

<u>Identification</u>**:**

- Run automated vulnerability scans
- Conduct a penetration test on organizational assets
- Conduct asset inventory
- Identify open findings by analyzing current version DISA STIGs and SRGs
- Cross reference Cyber.mil for new STIGs and SRGs
- Review vendor security bulletins
- Review documentation on requirements and industry standards
- Review threat intelligence reports

- Proactively check with the DoD VDP team to ensure no vulnerabilities have been reported within the organization.

Analysis & Reporting

- Conduct a business impact analysis / risk assessment for vulnerabilities that have not been automatically scored.

Remediation / Mitigation

- Create tasks for areas of responsibilities (AORs) to remediate vulnerabilities

Verification and Monitoring

- Compare successive vulnerability scans
- Review previous security controls assessments / audits

Definitions

Roles and responsibilities

Roles and their responsibilities have been identified and documented	A specific stakeholder has been assigned to each role	Roles and responsibilities adhere to rules, regulations, and best practices.
⃠	✓	✓

Definitions: Defining roles and their responsibilities prior to implementing the plan will avoid confusion and help to streamline the management process. It helps by enhancing communication and collaboration and narrows down any deficiencies in the management process.

Score Explanation: Roles and their respective responsibilities have been identified and documented. A stakeholder has been assigned to each role. There are no mandated roles for a vulnerability management team in the DoN; however, the *CRR Supplemental Resource Guide* mentions that the best practice is to organize the roles into 3 different categories.

Solution: Ensure that each role that has been outlined in the plan document is categorized by one or more of the following:

1) Monitoring role
2) Remediation role
3) Authorization role

Training requirements

Training requirements have been identified	Training requirements have been documented	Training requirements ensure team members are competent in their role	Training requirements adhere to rules, regulations, and best practices
✓	✓	✓	✓

Definition: The most important aspect of having clearly defined training requirements is that it helps to eliminate situations where an employee is filling a role that they aren't qualified to perform. Each role needs to be filled by someone who is competent in the tasks and activities associated with their role. Keeping a list of the training requirements, as well as a list of who is or isn't compliant with those requirements will help to improve audit readiness.

Score Explanation: All DoD and DoN mandated training requirements are tracked via the Audit Readiness team and are clearly defined in the internal *Security Awareness and Training Plan* document. This document cross references all the mandatory training requirements as outlined by the DoN and DoD.

Measures of Effectiveness

Measures of effectiveness have been defined & documented	Measures of effectiveness align with the overall goals of the VMP	Measures of effectiveness are quantifiable and scalable	Measures of effectiveness include a benchmark for comparison.	The time frame requirements for collecting relevant data have been defined and are reasonable
⃠	✓	✓	⊗	⃠

Definition: Having well defined measures of effectiveness is key to assessing the effectiveness of the vulnerability management program. All measures of effectiveness should align with the goals identified in the strategy, be quantifiable, scale with the size of the vulnerability processes, and be assessed in a timely manner. Most importantly, they should also include a benchmark, which serves as a goal for the organization to meet.

Score Explanation: Some measures of effectiveness have been identified but are not included in the plan document. These include vulnerabilities per host and the number of exploitable vulnerabilities categorized by criticality. While these are great metrics, they should also be accompanied by a specific quantifiable value for comparison, so that the organization is able to easily determine where they are in terms of meeting established goals. The time frame requirement for collecting the data and forming a report of these measures of effectiveness have been established but should be included in the plan document. Additional measures of effectiveness will be needed to learn more about the program's current state and identify any deficiencies.

Solution: Include a few more measures of effectiveness in the plan document. Some examples include average time to discovery, average time to remediation, scan coverage, false positives rate, and percentage of vulnerabilities found by automation vs. manually. Make sure to include what information is necessary for determining those metrics, a benchmark for comparing the metrics to, as well as how often the data should be collected and reported in the plan document.

Other definitions

Classifications for vulnerabilities have been defined	A remediation timeline for each vulnerability classification has been created	A process for revising the plan document has been defined	A schedule for reviewing the efficiency of the VMP has been defined	Communication Channels have been identified	The plan document contains an appendix
✓	✓	⊗	⊗	⊘	⊗

Definition: Defining additional details like terms, acronyms, review schedules, and processes for revising the document establishes clarity and consistency, therefore easing the readability and overall quality of the document.

Score Explanation: *DoD 8531.01* defines the vulnerability classification requirements for all DoD components. It mandates that each component uses the CVSS scoring system and associated remediation timelines, which the organization is currently doing. The organization's *Cyber Security Policy* document defines the approach to how they meet this requirement through implementing ACAS. There is no official process for revising the plan document. There is no periodic time requirement for how often the VMP should be analyzed to ensure that it is operating efficiently. Communication channels have been established and are enforced by the organization's leadership, but those communication channels should still be clearly defined in the plan document. The plan document does not contain an appendix.

Solution:

1) Include a process for revising the plan document.
2) Include a time requirement for how often the VMP should be analyzed to ensure it maintains efficiency and stays on track with rules, regulations, and best practices.
3) Include communication channels used by the VMP.
4) Include a sample appendix. This should include the following:
    a. Glossary of terms and Acronyms
    b. References
    c. Tables and Diagrams
    d. Version control information

Tools and Sources

Tools

Tools necessary for carrying out VMP activities have been identified	Tools selected are included in the plan document	The tools selected are approved by government authorizing officials.	The tools selected can easily be integrated into the VMP tasks and are reasonably easy to use	The tools selected have comprehensive coverage of VMP processes such as identification, assessment, and mitigation	The tools selected are within the established draft budget
✓	⊗	✓	✓	✓	✓

Definition: Tools aligned with each activity improve efficiency and effectiveness, especially if they involve automation. The organization needs to carefully select the tools appropriate for the job. Selecting one that isn't appropriate could have an adverse effect.

Score Explanation: The main tools used for vulnerability management within the organization such as SCC, eMASS, Policy Auditor, VRAM, and Nessus are all approved and required by the DoN and DoD. These tools are approved in the DISA approved product list, appropriate for the task, reasonably easy to use, and are cost effective. The tools are not listed in the plan document.

Solution: Include the tools necessary to perform each activity in the plan document. The table below is an example of how this might look.

SRG and STIG implementation	Vulnerability Scanning	Review vendor security bulletins	Penetration testing	Checking for new patches and STIGs	Report Development
SCC, STIG Viewer, Evaluate STIG	Nessus, VRAM, eMASS	Web Browser	Hping3, Nmap, BurpSuite, Hashcat.	Web Browser	Excel

Vulnerability Information Sources

Sources of vulnerability information have been identified	Sources of vulnerability information are approved by respective authorities within the organization	The sources identified provide information for all assets and environments in the organization
✓	✓	⊘

Definition: Carefully selecting your sources of vulnerability information is essential to accuracy, timeliness, consistency, and credibility. To mitigate those risks, the government has mandated the use of specific sources of vulnerability information. The vulnerability source also needs to be capable of integration into the automated assessment process to maintain SCAP compliance. The CRR Supplemental

Guide does not state that the sources need to be included in the plan document, but the organization should still maintain a separate list of sources.

Score Explanation: Sources of vulnerabilities have been chosen and are an approved and vetted method for gathering information. The organization maintains a list of these sources, but it doesn't have exhaustive coverage of every asset or product in the environment.

Solution: Continue adding more sources of vulnerabilities to the list until all the assets and products are covered.

Implementation

In this phase, the vulnerability management program will utilize the selected tools, processes, activities, and methodologies to identify, analyze, report, remediate/mitigate, and monitor vulnerabilities within the established timeframe requirements.

Training

Training

All key stakeholders are trained in their associated processes and tasks	A current record of training compliance is being maintained
⃠	✓

Definition: It isn't sufficient to only include the training requirements in the plan document. organizations need to ensure that their employees are maintaining compliance with the training requirements that were established. This means that a record of training compliance needs to be made, and it needs to be revisited on a frequent basis to ensure continuous compliance.

Score Explanation: There are no official training requirements for members of a vulnerability management team, but other requirements such as annual cyber security awareness, privileged user training, and other training requirements identified by the organization's training and awareness team are being met. A record of training is kept by the training and awareness team and is centrally managed. It is, however, suggested that each member of the VMP take the ACAS operator training, which not all team members have done yet.

Solution: Have each member of the VMP team take the DoD suggested training: ACAS Operator. It would also benefit the program to include some other forms of training that are not officially sponsored by the DoD but still give good insight into the vulnerability management lifecycle. The following are a few examples of training:

1) Shell Sharks Vulnerability Management Bootcamp – This free online blog walks you through each step in managing vulnerabilities and provides labs that allow you to gain some hands-on experience.
    - https://www.linkedin.com/learning/

2) Udemy & LinkedIn Learning courses – These two websites offer a wide array of vulnerability management courses.
    - https://www.udemy.com/
    - https://www.linkedin.com/learning/

Identification and Assessment

Identification & Assessment

Automated vulnerability scans are scheduled according to the frequency established in the plan document	Security Technical Implementation Guides are continuously reviewed and implemented	Internal penetration tests are being conducted.
✓	✓	⃠

Definition: The organization needs to ensure that they are implementing the methods of identification and assessment that have been outlined in the plan document. If some of the methods are not implemented correctly, or at all, there will not be a comprehensive coverage of vulnerabilities, effectively widening the attack surface.

Score Explanation: Although the internal VMP team is not responsible for the configuration and running the scans, it is still their responsibility to ensure that vulnerabilities are being identified. The VMP is fulfilling this responsibility by ensuring the ACAS team is running scans on a weekly basis and configuring the scans according to the established ACAS standard operating procedures and supplemental guides. According to section 4.7 of the organization's *Cybersecurity Policy* document, penetration tests are to be conducted on an ad-hoc basis on mission-owner systems, but it does not mention performing red team operations on internal assets. After speaking with the ISSM, it was clarified that internal penetration tests are not conducted, except for web-risk assessments, which involve only assets with a public facing URL.

Solution: The organization should consider performing internal penetration tests beyond that of web risk assessments, whenever financially viable.

Reporting and Remediation

Recording Vulnerabilities

Vulnerabilities are being recorded and reported according to DoD standards	The organization is implementing access controls on the vulnerability repository and other sources of vulnerability information
✓	✓

Definition: Recording vulnerabilities in a clear, consistent, and precise manner will improve readability and communication and make it easier to identify trends. By adhering to DoD and DoN recording and

reporting standards, the organization will be able to easily observe vulnerability trends internally. The organization should also ensure that the repository containing the internally recorded vulnerabilities has appropriate access controls. This ensures that unauthorized changes won't be made, which would disrupt vulnerability management operations.

The following are some recording and reporting requirements:

DoDI 8531.01: "DoD components will draft an analysis report to display the output of the vulnerability analysis. The analysis report must include one or more of the following: "

1. Name of the vulnerability
2. Date of discovery
3. Recommendation to correct the vulnerability
4. The CVSS score
5. The CVSS severity rating
6. Details of how the loss of confidentiality, integrity, or availability could affect DoD operations, organizational assets, or individuals

TASKORD 17-0019: Vulnerabilities will be remediated according to the following timeline:

1. Category 1: 21 days
2. Category 2: 45 days
3. Category 3: 60 days

Score Explanation: The organization is meeting each of the requirements listed above in *DoDI 8531.01* and *TASKORD 17-0019.*

Disposition

Methods for disposition of vulnerabilities are being chosen and recorded	Chosen methods of disposition are tested prior to deployment	Chosen methods of disposition are continuously tracked to ensure there is no abnormal or unwanted behavior
✓	✓	✓

Definition: Disposition actions are the methods for managing vulnerabilities, which vary depending on the nature of the asset. Some common risk dispositions involved with vulnerabilities include acceptance, avoidance, mitigation, and transference. From each of these, one can derive a disposition methodology for a vulnerability. For example, for risk transference, you can acquire a vendor-provided solution. Each disposition methodology chosen for a vulnerability should be documented alongside the vulnerability assessment. The chosen method must first be tested on a specifically selected group of assets before deploying the solution to the rest. Once deployed, the organization needs to continuously monitor for unwanted or abnormal changes to operations and revert the solution if necessary.

Score Explanation: Recommended actions (disposition actions) are recorded for each vulnerability. Recommended actions are given by the output of ACAS scans, the "fix text" section of DISA STIGs, and the reports of web risk assessments (WRAs). These recommended actions are assigned to each of the

respective areas of responsibility (AORs) for the data custodians to implement. The data custodians will deploy the solution to a test or development environment and monitor for any unwanted changes prior to deploying it to production. Once in production, they continue to monitor for any unwanted changes.

Root Cause Analysis

The organization is conducting root cause analysis to determine why vulnerabilities exist.	Corrective actions are being created to address the root cause of vulnerabilities.	The vulnerability repository is being updated to include the root cause analysis and corrective actions.
⃠	✓	✓

Definition: By seeking to understand why a vulnerability appears to begin with, the organization could prevent future vulnerabilities of a similar nature from occurring. Root cause analysis should be performed with the intent of trying to stop the vulnerability before it recurs or worsens.

Score Explanation: The internal VMP is working with AORs to determine the root cause of vulnerabilities but is doing so in an informal way. A formal technique for determining the root cause should be used. When root causes of vulnerabilities are identified, a JIRA task is created for data custodians to remediate the root cause. The VMP is also building a knowledge base for tracking root causes.

Solution: The organization should implement a formal process for discovering, documenting, and remediating the root cause of vulnerabilities. The following are a few defined techniques for root cause analysis:

Graphical methods: Fishbone diagrams, Issue Trees, Fault trees.

The 5 Whys method: Keep asking “Why?” until you’ve either reached what you believe is the root cause or you’ve asked “why?” 5 times. Example: A company’s database of PHI was leaked.

1) Why did the information leave the database? – It was exported by a remote user via SQL injection.
2) Why was the person able to use SQL injection? – The web app used outdated software, which did not correctly sanitize input.
3) Why was the code outdated? – Security updates were not regularly being applied.
4) Why were security updates not being regularly applied? – No one was aware that there was a software patch available.
5) Why was no one aware of the new software patches? – Vulnerability scans were not being conducted, and there was no formal process for patching.

Assessment and Improvement

Assessing the capabilities of the vulnerability management program is essential to knowing if pertinent processes are staying aligned with defined goals. This is when the organization collects relevant information and compares it to their measures of effectiveness. By doing this, the organization will continuously improve their vulnerability management program, thereby reducing their risk profile.

Collection and Analysis

Program Information Collection

Information is collected on processes outputs, policies, plans, guidelines, and strategy.	The information collected is relevant to improving the VMP	The information is gathered in accordance with the timeline established in the plan document
⃠	✓	⃠

Definition: Information needs to be collected to ensure that the VMP processes are aligned with the goals defined in the strategy development phase. The timeline for when to collect this information should be outlined in the plan document. When collecting program information to compare to the measures of effectiveness, the organization needs to ensure that the information collected is relevant and exhaustive.

Score Explanation: Relevant information is being collected from the output of processes and other sources of information, but more details are needed to better understand the effectiveness of the VMP. The collection of this information is a continuous effort, but there is no established timeline for when to collect information from other sources like policies, guidelines, etc.

Solution: Broadening the information collected will allow the VMP to include more measures of effectiveness in the weekly cyber security report. Examples of what information to collect for each of the suggested measures of effectiveness in the plan review are provided.

1. average time to discovery – Collect information about when vulnerabilities first enter a network, and when they are discovered.
2. average time to remediation – Collect information about when the vulnerabilities are first reported to AORs and when they are remediated.
3. false positives rate – Collect information about which vulnerabilities are determined to be false positives and true positives, as well as the age and accuracy of vulnerability information sources.

Program Information Analysis

The organization is comparing the defined measures of effectiveness with the program information collected	The organization is reevaluating the measures of effectiveness to determine if they are appropriate	Risks of not meeting measures of effectiveness and inaccurate assessments have been determined	An assessment report is created from the information analysis
⃠	⊗	⃠	✓

Definition: Now that the relevant information has been gathered concerning the operations of the VMP, that information needs to be compared to the defined measures of effectiveness. This analysis will help to determine whether the measures of effectiveness defined are providing actionable information and that they are keeping VMP operations aligned with their goals. During this time the organization must also determine the risks of not meeting those measure of effectiveness and create an assessment report to give to key stakeholders, which provides a clear picture of how efficiently the VMP is operating.

Score Explanation: So far, the only defined measures of effectiveness are what is included in the weekly cyber security report. Section 14.4 of the organization's Cyber Security Plan document states "On a recurring basis, the ISSM develops and promotes cybersecurity focused initiatives to address unacceptable vulnerability counts and past due POA&Ms to affecting systems," however, nowhere does it state what the unacceptable number of vulnerabilities is. Specific benchmarks will need to be identified to compare to the information collected. Once additional measures of effectiveness have been determined, they will need to be revisited to ensure that they are appropriate. The organization is aware of the risk of not meeting their measures of effectiveness but will need to provide more information once more are created.

Solution: For the organization to conduct a better analysis of their VMP, they will need to establish more measures of effectiveness. Measures of effectiveness are only valid when they can be compared to a defined threshold or historical data. For example, to have false positives rate as a measure of effectiveness, you will need to determine what the acceptable rate of false positives is or compare it to previous reports of false positives to identify trends. The VMP should also regularly review the plan document with information gathered to determine if all the requirements that have been defined are still being met, or if they need to be altered.

Improvement Efforts

Improvement

Deficiencies identified as defined by the measures of effectiveness are being addressed	The improvement process used is iterative and not finite
✓	✓

Definition: The organization should address any deficiencies identified during the information analysis.

Score Explanation: Even though the organization does not have as many measures of effectiveness as suggested, they are still addressing any deficiencies identified when comparing the information gathered with their measures of effectiveness. Each month the ISSM reviews the number of internal vulnerabilities

and determines if that number is acceptable. If not, he will work with the internal AORs to address the vulnerabilities themselves, or the root cause of the vulnerability.

Conclusion

Having a robust vulnerability management program enables an organization to address deficiencies and improve their defense capabilities, which results in reduced risk, optimized resources, and increased compliance. Since the internal vulnerability program within the organization is still new, there was a lack of insight into how well it was adhering to rules, regulations, and best practices and needed a comprehensive analysis of the program's current state to determine any deficiencies. The analysis of the internal vulnerability management program shows that it meets the standards for identifying, assessing, prioritizing, remediating, and validating the vulnerabilities internally, but additional attention is needed in the documentation and continuous improvements efforts.

How well does the program adhere to DoD mandates and guidelines?

- The organization has a strong adherence to DoD mandates and guidelines. By maintaining compliance with these mandates and guidelines, the organization is ensuring that they are detecting, preventing, and mitigating cyber-attacks.

How well does the program adhere to industry best practices?

- DoD rules and guidelines will almost always incorporate industry best practices. Reviewing the DoD instruction manuals will show that NIST publications such as *NIST 800-171* are usually used as a framework for constructing mandates. Since the organization has a strong adherence to DoD mandates, they are also incorporating many industries best practices into their vulnerability management processes. There are, however, some industry best practices that are not contained within DoD mandates. These involve the creation and iteration of vulnerability management programs from the point of their creation and into the continuous improvements phase. One major best practice that is not mandated by the DoD and could use further attention is making sure to start with strategy development and plan documentation before implementing any vulnerability management processes. By doing so, you essentially create guiding principles and a roadmap for which you can base your processes on, which keeps management operations aligned with organizational goals.

How well is the organization assessing the effectiveness of the internal vulnerability management program?

- More time will need to be spent on evaluating the effectiveness of the internal vulnerability management program. Assessing the program requires that you start by defining clear objectives, which were not explicitly documented. Measures of effectiveness are derived from the defined objectives and may have already existed but were not clearly identified in the plan document. These metrics need to be quantifiable, scalable, and a benchmark must exist for comparison. Without clearly defined measures of effectiveness, the organization will find it difficult to understand what information to gather, if resources are being used efficiently, and whether the program is effective and remaining relevant.

Ultimately, the internal vulnerability management program is performing well in terms of adhering to DoD mandates and industry standards. By doing so, they are ensuring that all internal assets are secured, and sensitive information is being protected. However, there is a shortcoming in the iteration of the program. Strategy and planning documentation are crucial elements when trying to determine the state of the program, and without it the organization cannot be sure that they have a clear insight into whether the information that is currently being collected and analyzed is relevant to organizational goals, and also what new information could be collected and used to their advantage. As the organization continues to iterate upon their strategy development and plan documentation, gaining this insight will start to become easier, allowing them to improve their vulnerability management capabilities.

References

Carnegie Melon University. (2016, December 17). *Vulnerability Management Version 1.1.* Cybersecurity and Infrastructure Security Agency. Retrieved from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/resources-tools/resources/cyber-resilience-review-supplemental-resource-guides

Chief of Naval Operations. (2023). *OPNAVINST 5239.* Office of the Chief of Naval Operations.

Joint Force Headquarters-Department of Defense Information Network. (2020). *TASKORD 17-0019 Assured Compliance Assessment Solution (ACAS) Operational Guidance.* Joint Force Headquarters-Department of Defense Information Network.

National Institute of Standards and Technology (NIST). (2020). *NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1.* NIST Research Library.

National Institute of Standards and Technology (NIST). (2022). *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology (NIST SP 800-40r4).* NIST Research Library.

REDACTED. (2024). *Cybersecurity Plan for REDACTED.*

REDACTED. (2024). *Vulnerability Management Plan for REDACTED.*

REDACTED. (2025). *Security Awareness and Training Plan for REDACTED.*

The Chief Information Officer of the Department of Defense (DoD). (2020). *DoD Instruction 8531.01, DoD Vulnerability Management.* The Department of Defense (DoD).