Software Engineering Institute

CERT® Resilience Management Model, Version 1.2

Vulnerability Analysis and Resolution (VAR)

Richard A. Caralli
Julia H. Allen
David W. White
Lisa R. Young
Nader Mehravari
Pamela D. Curtis

February 2016

CERT Program

http://www.cert.org/resilience/

Carnegie Mellon

This material is based upon work funded and supported by various entities under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0003234

VULNERABILITY ANALYSIS AND RESOLUTION

Operations

Purpose

The purpose of Vulnerability Analysis and Resolution is to identify, analyze, and manage vulnerabilities in an organization's operating environment.

Introductory Notes

A vulnerability is the susceptibility of an asset and associated service to disruption. Examples of vulnerabilities are weaknesses in the physical or technical infrastructure of the organization and flaws in the character of an individual employee. All assets of the organization that are operationally deployed—people, information, technology, and facilities—are subject to some level and type of vulnerability.

Vulnerabilities can result in operational risks and must be identified and remediated to avoid disruptions to the organization's ability to meet its strategic objectives. Vulnerability Analysis and Resolution is complementary to Risk Management. It requires that an organization identify weaknesses to its assets and services and understand the potential impact to the organization when these weaknesses are exploited.

As organizations have grown more dependent on their technical infrastructures, there has been a corresponding increase in focus on identifying only technical vulnerabilities. However, operational risk emanates from weaknesses in the protection of *all* types of assets, and thus the vulnerability analysis and resolution activity must cover not only weaknesses in the technical infrastructure but also potential threats to the viability of people, information, and facilities.

The identification and remediation of technical vulnerabilities are means for mitigating operational risk, but they do not fully constitute the activities of risk management. Instead, Vulnerability Analysis and Resolution informs the organization of threats that must be analyzed in the risk management process to determine whether they pose tangible risk to the organization based on its unique risk drivers, appetite, and tolerance. In turn, the risk management process informs vulnerability analysis and resolution processes to focus attention on the assets and services that are most critical to meeting strategic objectives.

The Vulnerability Analysis and Resolution process area describes the organization's ability to establish a vulnerability management strategy and to efficiently and effectively assign enterprise-wide resources to implement that strategy. The organization identifies and analyzes vulnerabilities across the enterprise and communicates relevant information about these vulnerabilities to other organizational processes that require this information. Strategies are developed to reduce the organization's exposure to vulnerabilities. In this way, the organization is mitigating risk where the exploited vulnerability has the potential to impact the organization.

Vulnerability Analysis and Resolution provides the organization an important opportunity to improve processes that may introduce vulnerabilities into the operating environment. Vulnerabilities are logged and tracked, and root-cause analysis and trending are performed on them to determine if breakdowns in other organizational processes are resulting in exposure. This knowledge is translated into improved strategies for protecting and sustaining assets and services as well as improvements in the processes.

Vulnerabilities may result in events and incidents that the organization must manage. *(The Incident Management and Control process area addresses the processes for identifying, analyzing, handling, and responding to incidents.)*

Vulnerability identification and analysis activities provide information about potential risks to the organization. *(Risks are identified, analyzed, and mitigated in the Risk Management process area.)*

Related Process Areas

The risk management cycle for organizational services, processes, and assets is addressed in the Risk Management process area.

Monitoring for events, incidents, and vulnerabilities is addressed in the Monitoring process area.

Summary of Specific Goals and Practices

Goals	**Practices**
VAR:SG1 Prepare for Vulnerability Analysis and Resolution	VAR:SG1.SP1 Establish Scope
	VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy
VAR:SG2 Identify and Analyze Vulnerabilities	VAR:SG2.SP1 Identify Sources of Vulnerability Information
	VAR:SG2.SP2 Discover Vulnerabilities
	VAR:SG2.SP3 Analyze Vulnerabilities
VAR:SG3 Manage Exposure to Vulnerabilities	VAR:SG3.SP1 Manage Exposure to Vulnerabilities
VAR:SG4 Identify Root Causes	VAR:SG4.SP1 Perform Root-Cause Analysis

Specific Practices by Goal

VAR:SG1 Prepare for Vulnerability Analysis and Resolution

Preparation for vulnerability analysis and resolution activities is conducted.

Preparation is conducted by establishing and maintaining a strategy for identifying, analyzing, and addressing vulnerabilities in the operational environment. This is typically documented in a vulnerability management plan. The vulnerability management strategy addresses the specific actions and management approach used to apply and control the vulnerability management activities within the organization. This includes scoping the operational environment to be scanned for potential vulnerabilities, the development of criteria to categorize the vulnerabilities, and the parameters used to identify, analyze, and potentially address vulnerabilities.

The operating environment of an asset consists of the physical or logical locations where the asset is deployed and the set of controls (administrative, technical, and physical) that are applied to that asset at that location.

VAR:SG1.SP1 Establish Scope

The assets and operational environments that must be examined for vulnerabilities are identified.

An asset and the services it supports are vulnerable to disruption if there is a weakness that is not currently remediated by an administrative, technical, or physical control. The universe of potential vulnerabilities in an organization's operational environment is almost limitless. The organization must therefore focus its vulnerability analysis and resolution activities toward identifying the vulnerabilities to the organization's most high-value assets and services. Otherwise, the organization can expend significant human and financial resources identifying vulnerabilities that have limited potential for posing operational risk to the organization.

The scoping activity establishes the ranges of assets that will be the focus of the organization's vulnerability analysis and resolution activities. The scoping activity should be driven by the resilience requirements of the identified assets.

Typical work products

1. Documented scope of vulnerability analysis and resolution activities

Subpractices

1. Identify the assets that are the focus of vulnerability analysis and resolution activities.

   The organization's high-value assets are identified in the Asset Definition and Management process area. Further prioritization is performed in other process areas for specific asset types: Human Resource Management (people), Knowledge and Information Management (information), Technology Management (technology), and Environmental Control (facilities).

   High-value assets should form the basis for the scope of vulnerability analysis and resolution activities. Deciding upon a proper scope, however, may also require an understanding of associated services and their value to supporting the organization's strategic objectives.

2. Identify the operational environments where vulnerabilities may exist for each asset.

   This will vary depending upon the type of asset under examination:

   - For an information asset, the operational environment will depend on where the asset is physically contained (in a file room or on a server) and on the form of the asset (paper or electronic).
   - For a technology asset, the operational environment includes where the asset is located physically (e.g., at a data center, in a server farm) and to what other assets it is connected (e.g., to a network).
   - For a facilities asset, the operational environment includes the physical and geographical location of the asset and its proximity to other organizational assets.

   The organization must prioritize the operational environments on which to focus vulnerability analysis and resolution activities to the highest benefit to the organization.

VAR:SG1.SP2 Establish a Vulnerability Analysis and Resolution Strategy

An operational vulnerability analysis and resolution strategy is established and maintained.

A comprehensive vulnerability management strategy addresses items such as

- the determination and documentation of the scope of vulnerability analysis and resolution
- a plan for performing vulnerability analysis and resolution
- resources and accountability for vulnerability identification and remediation
- approved methods and tools to be used for the identification, analysis, remediation, monitoring, and communication of vulnerabilities
- a process for organizing, categorizing, comparing, and consolidating vulnerabilities
- thresholds for remediation and resolution activities
- time intervals for vulnerability identification and monitoring activities

The vulnerability analysis and resolution strategy should be guided by the risk criteria and tolerances of the organization and is often documented in an organizational vulnerability analysis and resolution plan. This plan should support and be developed along with the organization’s risk management plan. The strategy is reviewed with relevant stakeholders to promote commitment and understanding.

Typical work products

1. Vulnerability analysis and resolution strategy
2. Vulnerability analysis and resolution plan
3. List of appropriate tools, techniques, and methods for identifying vulnerabilities

Subpractices

1. Develop and document an operational vulnerability analysis and resolution strategy.

   The strategy for addressing vulnerability analysis and resolution should be documented in a plan that can be communicated to relevant stakeholders and implemented. The plan should address

   - the scope of vulnerability analysis and resolution activities
   - the essential activities that are required for vulnerability analysis and resolution
   - a plan for collecting the data necessary for vulnerability activities
   - tools, techniques, and methods that have been approved for identifying and analyzing vulnerabilities across a range of assets
   - a schedule for performing vulnerability activities
   - the roles and responsibilities necessary to carry out the plan

- the skills and training required to perform the vulnerability analysis and resolution strategy and plan
- the relative costs associated with the activities, particularly for the purchase and licensing of tools, techniques, and methods
- relevant stakeholders of the vulnerability activities and their roles
- objectives for measuring when the plan and strategy are successful

2. Communicate the operational vulnerability analysis and resolution strategy to relevant stakeholders and obtain their commitment to the activities described in the strategy.

   Several operational resilience management processes rely on the types of information that will result from the vulnerability analysis and resolution process. Processes such as risk management, incident management and control, and service continuity should be considered as areas where regular communications about vulnerability activities and actual vulnerabilities would be necessary.

3. Assign resources to specific vulnerability analysis and resolution roles and responsibilities.
4. Identify the tools, techniques, and methods that the organization will use to identify vulnerabilities to assets.

   The organization should compile a list of approved and recommended tools, techniques, and methods that can be used for vulnerability activities. Pre-approving tools, techniques, and methods ensures consistency and cost effectiveness, as well as validity of results. This list should cover the entire range of assets and include both procedural and automated methods.

VAR:SG2 Identify and Analyze Vulnerabilities

A process for identifying and analyzing vulnerabilities is established and maintained.

The identification and analysis of vulnerabilities are essential elements of managing vulnerabilities *before* they are exploited. Information learned through the identification of vulnerabilities is contextualized using enterprise risk information.

VAR:SG2.SP1 Identify Sources of Vulnerability Information

The sources of vulnerability information are identified.

Information about potential vulnerabilities is available from a wide variety of organizational and external sources. External or public sources typically provide information that is focused on common technologies that are used by a wide range of organizations. Internal sources typically provide information about vulnerabilities that are unique to the organization and range across all types of assets, including people, information, and facilities. Internal sources of vulnerability information are often generated by other operational resilience management processes such as incident management and monitoring, or through IT service delivery and operations processes such as the service desk and problem management. These sources may provide information about vulnerabilities that the organization has observed or that have been exploited, resulting in disruption to the organization.

These are examples of sources of vulnerability data:

- vendors of software, systems, and hardware technologies that provide warnings on vulnerabilities in their products
- common free catalogs, such as the US-CERT Vulnerability Notes Database and the MITRE Corporation's Common Vulnerabilities and Exposures list
- industry groups
- vulnerability newsgroups and mailing lists
- the results of executing automated tools, techniques, and methods
- internal processes such as service desk, problem management, incident management and control, and monitoring, where vulnerabilities may be detected

Vulnerability data collection is a continuous process. Expanding the sources of vulnerability information helps the organization improve its identification of vulnerabilities in a timely manner and extends the organization's awareness of an expanding range of vulnerability types. The organization must ensure that as new vulnerability information sources become available they are incorporated into the organization's vulnerability repository and corresponding identification and analysis activities.

Typical work products

1. List of sources of vulnerability information

Subpractices

1. Identify sources of relevant vulnerability information.

   The sources of vulnerability information should fit the organization's vulnerability identification and analysis needs. The internal sources of vulnerability information supplied by other operational resilience management processes should be included in the list.

2. Review sources on a regular basis and update as necessary.

   New sources of vulnerability information are continually emerging. The organization must review these sources and add them to its source list to be sure to have access to the most current, accurate, and extensive information about vulnerabilities.

VAR:SG2.SP2 Discover Vulnerabilities

A process is established to actively discover vulnerabilities.

Vulnerabilities are discovered from active review and capture from the organization's standard list of sources of vulnerability information. There are many techniques that an enterprise can use to discover vulnerabilities. These include

- performing internal vulnerability audits or assessments (using tools, techniques, and methods)
- performing external-entity assessments
- reviewing the results of internal and external audits

- periodically reviewing vulnerability catalogs, such as the US-CERT Vulnerability Notes Database and the MITRE Corporation’s Common Vulnerabilities and Exposures list
- subscribing to vendor notification services
- subscribing to vulnerability notification services (mailing lists)
- reviewing reports from industry groups
- reviewing vulnerability newsgroups
- using lessons-learned databases, such as the incident knowledgebase *(The incident knowledgebase is addressed in the Incident Management and Control process area.)*
- monitoring high-value organizational processes and infrastructure *(Monitoring for events, incidents, and vulnerabilities is addressed in the Monitoring process area.)*
- using reports of vulnerabilities from other processes such as the organization’s service desk or the problem management process

The organization establishes a vulnerability repository as the central source of vulnerability life-cycle information. As vulnerabilities are discovered, they are submitted to the organization’s vulnerability repository by capturing the information in a format that is usable in the organization’s vulnerability identification and analysis process. The repository is an essential construct that is vital to the efficiency and effectiveness of other operational resilience management processes. For example, accurate, complete, and timely information about vulnerabilities can assist in the examination of incidents and events, provide threat information to the risk management process for the identification of risks, and form the basis for root-cause analysis and trending for overall improvement of the operational resilience management system.

Vulnerability identification is a continuous activity. Some techniques for identifying vulnerability information are performed on a discrete basis, while others, such as monitoring, are more continuous. For discrete activities, the organization must decide the appropriate time intervals that it will use to repeat the identification activities to ensure that it has the most current and accurate information in its vulnerability repository.

Typical work products

1. Vulnerability data and information
2. Vulnerability repository

Subpractices

1. Discover vulnerabilities.

   Data collection should be coordinated to discover vulnerabilities and populate the vulnerability repository as efficiently as possible.

   These are examples of source documents from which vulnerabilities are discovered:

   - reports from assessment tools and methods
   - audit reports

- vulnerability databases
- emails from mailing lists
- vulnerability reports (from vulnerability databases)
- vendor notifications
- newsgroup messages
- incident knowledgebase
- communications from monitoring processes
- service desk or problem management reports

2. Provide training to staff to perform data collection and discover vulnerabilities.

   Individuals involved in the vulnerability discovery process should be skilled and trained in the use of appropriate tools, techniques, and methodologies. They should have access to the sources of vulnerabilities, including automated tools. Where automated tools are involved, the organization should ensure that training is provided on the appropriate and secure use of the tools.

3. Populate the vulnerability repository.

   Basic information that should be collected about vulnerabilities includes

   - a unique organizational identifier for internal reference
   - description of the vulnerability
   - date entered into the repository
   - references to the source of the vulnerability
   - the importance of the vulnerability to the organization (critical, moderate, etc.)
   - individuals or teams assigned to analyze and remediate the vulnerability
   - a log of remediation actions taken to reduce or eliminate the vulnerability

   The vulnerability repository is a source of risk to the organization if accessed by unauthorized individuals. The organization should apply access controls to the vulnerability repository to permit only authorized individuals to view, modify, or delete information.

4. Provide access to the vulnerability repository to appropriate process stakeholders.

VAR:SG2.SP3 Analyze Vulnerabilities

Vulnerabilities are analyzed to determine whether they have to be reduced or eliminated.

The mere identification of a vulnerability is not sufficient for determining whether the organization should act to counter it. With the number of vulnerabilities growing exponentially (particularly for technology assets), no organization can (or would want to) address all of them. The organization must analyze vulnerabilities to determine which ones require additional attention.

Through vulnerability analysis, the organization seeks to understand the potential threat that the vulnerability represents. The structure of the vulnerability—what it can do, how it is exploited, the potential effects—must be carefully considered in the context of the potentially affected assets and services. Vulnerability analysis includes activities to

- understand the threat and exposure
- review trend information to determine whether the vulnerability has existed before and what actions were taken to reduce or eliminate it
- identify and understand underlying causes for exposure to the vulnerability
- prioritize and categorize vulnerabilities for appropriate action to reduce or eliminate them
- refer vulnerabilities to the organization's risk management process when more extensive consideration of the impact of the potential threat must be performed to determine an appropriate mitigation strategy

As a result of analysis, some vulnerabilities will be determined to be of no relevance to the organization (i.e., the organization is not exposed to them or the exposure is negligible). Other vulnerabilities will have to be addressed through a simple fix (such as a software patch or by turning off unnecessary services), and some will have to have a formal strategy developed. The organization should assign a course of action to each vulnerability.

Typical work products

1. Vulnerability prioritization guidelines
2. Vulnerability analysis
3. List of vulnerabilities prioritized for disposition
4. Updated vulnerability repository

Subpractices

1. Develop prioritization guidelines for vulnerabilities.

   Prioritization guidelines should help the organization to sort and prioritize vulnerabilities consistently according to their relevance to the organization. The relevance to the organization may be characterized either in qualitative terms (high, medium, or low) or quantitative terms (through a numerical scale). The prioritization will provide the organization a structured means for determining the appropriate categorization for resolution actions.

2. Analyze the structure and action of the vulnerability.

   This may require the vulnerability to be decomposed into other artifacts such as threat, threat actor, motive, and potential outcome. In addition, relationships between vulnerabilities may be identified that could indicate similar root causes or origins that must be considered in resolution actions.

3. Prioritize and categorize vulnerabilities for disposition.

Based on the organization's prioritization guidelines and the results of vulnerability analysis, vulnerabilities must be categorized by disposition.

These are examples of categories for vulnerability resolution:

- Take no action; ignore.
- Fix immediately (typically the case for vendor updates or changes).
- Develop and implement vulnerability resolution strategy (typically the case when the resolution is more extensive than simple actions such as vendor updates).
- Perform additional research and analysis.
- Refer the vulnerability to the risk management process for formal risk consideration.

Vulnerabilities that are referred to the risk management process are typically those that cannot be resolved without more extensive decomposition and consideration of organizational consequences and impact.

4. Update the vulnerability repository with analysis and prioritization and categorization information.

VAR:SG3 Manage Exposure to Vulnerabilities

Strategies are developed to manage exposure to identified vulnerabilities.

Vulnerability resolution is the action that the organization takes to reduce or eliminate exposure to a vulnerability. It is the result of vulnerability analysis and prioritization.

Vulnerability resolution can also be a type of risk management activity. The actions to eliminate or reduce exposure to a vulnerability can be an outcome of the organization's formal risk management process, which is typically much more extensive than vulnerability analysis and resolution because it includes formal consideration of the organization's risk tolerances and the context of organizational consequence and impact.

In some cases, vulnerability resolution is relatively simple. Technical vulnerabilities posted on common vulnerability databases often include information about patching software, systems, firmware, or networks to reduce or eliminate vulnerabilities. Other types of vulnerabilities, including safety concerns for people or physical threats to facilities, may take more analysis and strategy development to address.

Vulnerability resolution may also extend beyond exposure reduction or elimination. Often, operational workarounds are necessary to avoid exposure to vulnerabilities when reduction or elimination is not possible.

VAR:SG3.SP1 Manage Exposure to Vulnerabilities

Strategies are developed and implemented to manage exposure to identified vulnerabilities.

The organization must develop and implement an appropriate resolution strategy for vulnerabilities to which the organization has determined that exposure must be reduced or eliminated. This strategy can include actions to

- minimize the organization's exposure to the vulnerability (by reducing the likelihood that the vulnerability will be exploited)

- eliminate the organization’s exposure to the vulnerability (by eliminating the threat, the threat actor, and/or the motive)

Managing exposure to vulnerabilities will likely require a consideration of these actions and the ways that they can be realized through the development and implementation of appropriate strategies. Strategies may span a wide range of activities, including

- implementing software, systems, and firmware patches
- developing and implementing operational workarounds
- developing and implementing new protective controls, or updating existing controls
- developing and implementing new service continuity plans, or updating existing plans

The organization must also consider the need to integrate managing exposure to vulnerabilities with other related organizational processes such as change management, configuration management, product acquisition, and monitoring.

Strategies for managing exposure may also require a consideration of the impact of the action against the continuing operations of the organization. For example, to reduce exposure to a vulnerability, the organization may be required to turn off or eliminate certain operating system services that staff members may need to perform their job functions. The organization must either determine a workaround to the loss of this service or allow the service to continue operating with the implementation of detective controls (such as audit logging and tracking) to ensure that it is not (or has not been) exploited by threat actors. Thus the organization’s strategy may include the development and documentation of the workaround or the types and extent of detective controls that will be implemented.

Once the organization has developed a vulnerability management strategy, it must be monitored to ensure effective implementation and the achievement of results as documented in the strategy.

Typical work products

1. Vulnerability management strategies
2. Updated vulnerability repository, with resolution status information
3. Vulnerability management strategy status reports

Subpractices

1. Develop a vulnerability management strategy for all vulnerabilities that require resolution.

   The organization may choose to address vulnerabilities that do not require extensive analysis without extensive strategy development. Typically, these vulnerabilities include those identified by software vendors or vulnerability databases for which a solution is readily available.

   For vulnerabilities that require further analysis and consideration, the organization should document a strategy for implementation. The strategy should address the actions that the organization will take to reduce or eliminate exposure or to provide an operational workaround if preferable. The strategy should detail the staff who are responsible for implementing and monitoring the strategy, the time period for performance, the cost of the strategy, and other relevant details.

If the vulnerability strategy requires more extensive involvement of the risk management process, it should be replaced by the development of risk mitigation strategies. *(The development of these strategies is addressed in the Risk Management process area.)*

2. Ensure that relevant stakeholders are informed of resolution activities.
3. Update the vulnerability repository with information about the vulnerability management strategy.
4. Monitor the status of open vulnerabilities.
5. Analyze the effectiveness of vulnerability management strategies to ensure that objectives are achieved.

VAR:SG4 Identify Root Causes

The root causes of vulnerabilities are examined to improve vulnerability analysis and resolution and reduce organizational exposure.

Organizations should identify, analyze, and resolve vulnerabilities as they are detected, but it is also necessary to perform more intensive analyses to understand how vulnerabilities originate and are related to each other. This provides the organization a powerful tool in proactively preventing future exposures.

Learning from vulnerability analysis and resolution activities involves performing root-cause analysis and translating vulnerability knowledge into actionable means for improving operational resilience.

VAR:SG4.SP1 Perform Root-Cause Analysis

A review of identified vulnerabilities is performed to determine and address underlying causes.

Root-cause analysis is a general approach for determining the underlying causes of events or problems as a means for addressing the symptoms of such events or problems as they manifest in organizational disruptions. Few vulnerabilities have organic causes (i.e., emerge on their own); instead, they are typically created by other actions or inactions such as poor software design, failure of organizational policies and processes, improper training, or operational complexity. Performing root-cause analysis allows the organization to look further into the reasons why exposures are occurring and to determine how to address these issues before they result in vulnerabilities that have to be analyzed and resolved.

A primary activity in root-cause analysis is to determine how to eliminate or reduce the underlying cause of exposures. Root-cause analysis may result in the development of strategies to address the root causes that are identified. As with developing strategies for managing vulnerabilities, this may include developing or improving controls as well as strategies for sustaining assets and services. It may also result in updating resilience training and awareness activities to ensure understanding of root causes and elimination of practices and processes that result in exposures. Overall, the identification and resolution of root causes can be used to improve the organization’s operational resilience by ensuring that lessons learned are translated to knowledge.

Many tools and techniques for root-cause analysis exist. The organization must familiarize itself with these tools and techniques, select those that are most appropriate for use, and provide training to relevant staff in their use.

Typical work products

1. Root-cause analysis reports
2. Updated vulnerability repository, with root-cause analysis

Subpractices

1. Identify and select root-cause tools, techniques, and methods appropriate for use in analyzing the underlying causes of vulnerabilities.
2. Identify and analyze the root causes of vulnerabilities.
3. Develop and implement strategies to address root causes.
4. Monitor the effects of implementing strategies to address root causes.

Elaborated Generic Practices by Goal

Refer to the Generic Goals and Practices document in Appendix A for general guidance that applies to all process areas. This section provides elaborations relative to the application of the Generic Goals and Practices to the Vulnerability Analysis and Resolution process area.

VAR:GG1 Achieve Specific Goals

The operational resilience management system supports and enables achievement of the specific goals of the Vulnerability Analysis and Resolution process area by transforming identifiable input work products to produce identifiable output work products.

VAR:GG1.GP1 Perform Specific Practices

Perform the specific practices of the Vulnerability Analysis and Resolution process area to develop work products and provide services to achieve the specific goals of the process area.

Elaboration:

Specific practices VAR:SG1.SP1 through VAR:SG4.SP1 are performed to achieve the goals of the vulnerability analysis and resolution process.

VAR:GG2 Institutionalize a Managed Process

Vulnerability analysis and resolution is institutionalized as a managed process.

VAR:GG2.GP1 Establish Process Governance

Establish and maintain governance over the planning and performance of the vulnerability analysis and resolution process.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the vulnerability analysis and resolution process.

Subpractices

1. Establish governance over process activities.

   Elaboration:

   Governance over the vulnerability analysis and resolution process may be exhibited by

   - developing and publicizing higher level managers' objectives and requirements for the process
   - sponsoring process policies, procedures, standards, and guidelines
   - oversight over the establishment, implementation, and maintenance of the organization's internal control system for the process
   - making higher level managers aware of applicable compliance obligations related to the process, and regularly reporting on the organization's satisfaction of these obligations to higher level managers
   - sponsoring and funding process activities
   - aligning vulnerability data collection and distribution activities with identified resilience needs and objectives and stakeholder needs and requirements
   - verifying that the process supports strategic resilience objectives and is focused on the assets and services that are of the highest relative value in meeting strategic objectives
   - regular reporting from organizational units to higher level managers on vulnerability analysis and resolution activities and results
   - creating dedicated higher level management feedback loops on decisions about the process, and recommendations for prioritizing process requirements and improving the process
   - providing input on identifying, assessing, and managing operational risks related to identified vulnerabilities for all asset types (people, information, technology, and facilities)
   - providing access to legal or other appropriate counsel to provide guidance on potential liabilities resulting from identified vulnerabilities
   - conducting regular internal and external audits and related reporting to audit committees on process effectiveness
   - creating formal programs to measure the effectiveness of process activities, and reporting these measurements to higher level managers

2. Develop and publish organizational policy for the process.

Elaboration:

The vulnerability analysis and resolution policy should address

- responsibility, authority, and ownership for performing process activities
- information categorization, labeling, and handling
- protection against tampering or unauthorized access
- encryption, secure storage, and secure transport and distribution of information
- procedures, standards, and guidelines for
  - identifying the assets that are the focus of vulnerability analysis and resolution activities
  - storage capacity of collection mechanisms and actions to take if capacity is exceeded by type of media
  - collection of vulnerability data
  - recording and storage of vulnerability data, including collection media (electronic logs, data files, databases, and information repositories)
  - distribution of vulnerability data, including media, methods, and channels
  - service level agreement terms and conditions for external entities involved in process activities
- methods for measuring adherence to policy, exceptions granted, and policy violations

VAR:GG2.GP2 Plan the Process

Establish and maintain the plan for performing the vulnerability analysis and resolution process.

Elaboration:

The plan for the vulnerability analysis and resolution process should not be confused with the organizational vulnerability analysis and resolution strategy and plan for identifying and analyzing vulnerabilities as described in specific practice VAR:SG1.SP2. The plan for the vulnerability analysis and resolution process details how the organization will perform vulnerability analysis and resolution, including the development of strategies and plans for vulnerability analysis and resolution.

Subpractices

1. Define and document the plan for performing the process.

   Elaboration:

   Special consideration in the plan may have to be given to the range of assets, asset types, and asset values (and related services) that are the focus of the vulnerability analysis and resolution activities. These activities help determine the scope of the vulnerability analysis and resolution activities that have the greatest potential to pose operational risks to the organization’s assets and services.

2. Define and document the process description.
3. Review the plan with relevant stakeholders and get their agreement.
4. Revise the plan as necessary.

VAR:GG2.GP3 Provide Resources

Provide adequate resources for performing the vulnerability analysis and resolution process, developing the work products, and providing the services of the process.

Elaboration:

The diversity of activities required to analyze and resolve vulnerabilities for all asset types requires an extensive level of organizational resources and skills and a significant number of external resources. In addition, these activities require a major commitment of financial resources (both expense and capital) from the organization.

Staff assigned to the vulnerability analysis and resolution process must have appropriate knowledge of the assets being examined and the objectivity to perform vulnerability analysis and resolution activities without concern for personal detriment and without the expectation of personal benefit.

Subpractices

1. Staff the process.

   Elaboration:

   These are examples of staff required to perform the vulnerability analysis and resolution process:

   - staff responsible for
     - collecting, analyzing, and prioritizing process requirements based on strategic objectives, business needs, and stakeholder requirements and needs
     - developing vulnerability analysis and resolution plans and programs and ensuring they are aligned with stakeholder requirements and needs
     - establishing an appropriate infrastructure for vulnerability data collection, recording, and distribution
     - vulnerability data collection, recording, distribution, and storage (associated with both electronic and physical assets)
     - vulnerability data protection and security (associated with both electronic and physical assets), so as to ensure data confidentiality, integrity, and availability
     - managing external entities that have contractual obligations for vulnerability analysis and resolution activities
   - owners and custodians of high-value services and assets that support the accomplishment of operational resilience management objectives
   - internal and external auditors responsible for reporting to appropriate committees on process effectiveness and the adequacy of collected data to accurately track the performance of operational resilience management processes

   Refer to the Organizational Training and Awareness process area for information about training staff for resilience roles and responsibilities.

   Refer to the Human Resource Management process area for information about acquiring staff to fulfill roles and responsibilities.

2. Fund the process.

   Refer to the Financial Resource Management process area for information about budgeting for, funding, and accounting for vulnerability analysis and resolution.

3. Provide necessary tools, techniques, and methods to perform the process.

   Elaboration:

   These are examples of tools, techniques, and methods to support the vulnerability analysis and resolution process:

   - methods, techniques, and tools for the identification, analysis, remediation, monitoring, and communication of vulnerabilities for all asset types
   - vulnerability data recording and storage methods, techniques, and tools (associated with both electronic and physical assets), including developing, populating, and maintaining the vulnerability repository
   - vulnerability data protection and security methods, techniques, and tools, including those necessary to ensure data confidentiality, integrity, and availability (associated with both electronic and physical assets)
   - vulnerability data distribution methods, techniques, and tools
   - methods, techniques, and tools for developing and managing collection media
   - tools for developing and maintaining traceability between stakeholder requirements and process requirements, plans, and programs

VAR:GG2.GP4 Assign Responsibility

Assign responsibility and authority for performing the vulnerability analysis and resolution process, developing the work products, and providing the services of the process.

Elaboration:

Specific practice VAR:SG1.SP2 calls for documenting the roles and responsibilities necessary to carry out the vulnerability analysis and resolution plan, as well as the roles of relevant stakeholders.

Refer to the Human Resource Management process area for more information about establishing resilience as a job responsibility, developing resilience performance goals and objectives, and measuring and assessing performance against these goals and objectives.

Subpractices

1. Assign responsibility and authority for performing the process.

2. Assign responsibility and authority for performing the specific tasks of the process.

   Elaboration:

   Responsibility and authority for performing vulnerability analysis and resolution tasks can be formalized by

   - defining roles and responsibilities in the process plan to include roles responsible for collecting, recording, distributing, and ensuring the confidentiality, integrity, and availability of vulnerability data
   - including process tasks and responsibility for these tasks in specific job descriptions

- setting policy requiring organizational unit managers, line of business managers, project managers, and asset and service owners and custodians to participate in and derive benefit from the process for assets and services under their ownership or custodianship
- including process tasks in staff performance management goals and objectives, with requisite measurement of progress against these goals
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing process tasks on outsourced functions
- including process tasks in measuring performance of external entities against contractual instruments

3. Confirm that people assigned with responsibility and authority understand it and are willing and able to accept it.

VAR:GG2.GP5 Train People

Train the people performing or supporting the vulnerability analysis and resolution process as needed.

Refer to the Organizational Training and Awareness process area for more information about training the people performing or supporting the process.

Refer to the Human Resource Management process area for more information about inventorying skill sets, establishing a skill set baseline, identifying required skill sets, and measuring and addressing skill deficiencies.

Subpractices

1. Identify process skill needs.

Elaboration:

These are examples of skills required in the vulnerability analysis and resolution process:

- knowledge of tools, techniques, and methods used to identify, analyze, remediate, monitor, and communicate vulnerabilities for all asset types, including those necessary to perform the process using the selected methods, techniques, and tools identified in VAR:GG2.GP3 subpractice 3
- knowledge of tools, techniques, and methods necessary to ensure the confidentiality, integrity, and availability of vulnerability data
- knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective process requirements, plans, and programs
- knowledge necessary to analyze and prioritize process requirements
- knowledge necessary to interpret vulnerability data and represent it in ways that are meaningful and appropriate for managers and stakeholders

2. Identify process skill gaps based on available resources and their current skill levels.

3. Identify training opportunities to address skill gaps.

Elaboration:

These are examples of training topics:

- operating, monitoring, and configuring tools, including the vulnerability repository
- supporting stakeholders in understanding and interpreting vulnerability data
- vulnerability data collection, recording, distribution, and storage techniques and tools
- securing data collected from system components to ensure data confidentiality, integrity, and availability
- working with external entities that have responsibility for process activities
- using process methods, tools, and techniques, including those identified in VAR:GG2.GP3 subpractice 3

4. Provide training and review the training needs as necessary.

VAR:GG2.GP6 Control Work Products

Place designated work products of the vulnerability analysis and resolution process under appropriate levels of control.

Elaboration:

These are examples of vulnerability analysis and resolution work products placed under control:

- vulnerability data
- process strategy and plans, including the scope of the plans and commitments to the plans
- list of sources of vulnerability information
- list of internal and external stakeholders and a plan for their involvement
- vulnerability prioritization guidelines
- prioritized process requirements, accepted requirements, and risks resulting from unsatisfied requirements
- infrastructure requirements
- vulnerability data collection and storage standards and parameters
- vulnerability data identification, monitoring, collection, analysis, remediation, handling, and storage methods, procedures, techniques, and tools
- vulnerability data distribution plans, procedures, processes, media, methods, and tools
- collection media, including electronic logs, data files, databases, and repositories
- vulnerability status reports, including resolution strategies
- policies and procedures
- contracts with external entities

VAR:GG2.GP7 Identify and Involve Relevant Stakeholders

Identify and involve the relevant stakeholders of the vulnerability analysis and resolution process as planned.

Elaboration:

Several VAR-specific practices address the involvement of stakeholders in the vulnerability analysis and resolution process. For example, VAR:SG1.SP2 calls for reviewing the vulnerability analysis and resolution strategy with stakeholders to promote understanding and gain commitment, VAR:SG2.SP2 calls for providing stakeholder access to the vulnerability repository, and VAR:SG3.SP1 requires that stakeholders be informed of vulnerability resolution activities.

Subpractices

1. Identify process stakeholders and their appropriate involvement.

   Elaboration:

   These are examples of stakeholders of the vulnerability analysis and resolution process:

   - higher level managers responsible for establishing organizational risk criteria and tolerances
   - staff responsible for the organization's risk management plan
   - asset owners, custodians, and users
   - staff responsible for managing operational risks to assets
   - staff responsible for establishing, implementing, and maintaining an internal control system for assets
   - staff responsible for developing, testing, implementing, and executing service continuity plans
   - external entities responsible for managing high-value assets and providing essential services
   - internet service providers
   - human resources (for people assets)
   - legal counsel
   - information technology staff, such as system administrators and CSIRTs
   - staff responsible for physical security (for facility assets)
   - internal and external auditors
   - owners of operational resilience management processes, including risk management, incident management and control, and service continuity

   Stakeholders are involved in various tasks in the vulnerability analysis and resolution process, such as

   - reviewing the process strategy and committing to the activities described in the strategy
   - establishing that plans (including the process plan) reflect the strategy
   - making decisions about process scope and activities
   - establishing requirements for the process
   - establishing vulnerability prioritization guidelines
   - assessing collected vulnerability data, including the vulnerability repository
   - providing feedback to those responsible for providing the vulnerability data on which the analysis results depend

- reviewing and appraising the effectiveness of process activities
- resolving issues in the process

2. Communicate the list of stakeholders to planners and those responsible for process performance.
3. Involve relevant stakeholders in the process as planned.

VAR:GG2.GP8 Measure and Control the Process

Measure and control the vulnerability analysis and resolution process against the plan for performing the process and take appropriate corrective action.

Refer to the Monitoring process area for more information about the collection, organization, and distribution of data that may be useful for measuring and controlling processes.

Refer to the Measurement and Analysis process area for more information about establishing process metrics and measurement.

Refer to the Enterprise Focus process area for more information about providing process information to managers, identifying issues, and determining appropriate corrective actions.

Subpractices

1. Measure actual performance against the plan for performing the process.
2. Review accomplishments and results of the process against the plan for performing the process.

Elaboration:

These are examples of metrics for the vulnerability analysis and resolution process:

- percentage of high-value assets (by type or category) subject to VAR process activities (This is determined by the resilience requirements associated with assets and assumes an up-to-date asset inventory *[refer to ADM]*.)
- percentage of high-value assets that have been monitored for vulnerabilities within an agreed-upon time interval
- percentage of high-value assets that have been audited or assessed for vulnerabilities
- percentage of reported vulnerabilities (by asset type or category) that require some form of resolution or remediation (course of action, reduction, elimination)
- percentage of vulnerabilities that have been satisfactorily remediated
- percentage of open vulnerabilities
- percentage of vulnerabilities that require resolution for which a vulnerability management strategy exists
- percentage of vulnerabilities with vulnerability management strategies that are on track per plan
- percentage of vulnerabilities requiring a root-cause analysis

- number of vulnerabilities that result in incidents for which a root-cause analysis was not performed
- number of vulnerabilities referred to the incident management and control process
- number of vulnerabilities referred to the service continuity process
- elapsed time from high-value vulnerability data collection to data distribution to key stakeholders
- number of vulnerabilities referred to the risk management process

percentage of organizational units, lines of business, and services using vulnerability data to assess the performance of operational resilience management processes

3. Review activities, status, and results of the process with the immediate level of management responsible for the process and identify issues.

Elaboration:

Periodic reviews of the vulnerability analysis and resolution process are needed to ensure that

- current sources of vulnerability data are in use
- assets subject to the process are identified, documented, and included in the scope of process activities
- assets that have been retired are removed from the scope of the process
- vulnerability data is identified, collected, and stored in a timely manner
- the vulnerability repository is established and maintained
- access to the vulnerability repository is limited to authorized staff
- vulnerability management status reports are provided to appropriate stakeholders in a timely manner
- vulnerabilities are referred to the risk management process when necessary
- actions requiring management involvement are elevated in a timely manner
- performance of process activities is being monitored and regularly reported
- key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports
- administrative, technical, and physical controls are operating as intended
- controls are meeting the stated intent of the resilience requirements
- actions resulting from internal and external audits are being closed in a timely manner

4. Identify and evaluate the effects of significant deviations from the plan for performing the process.

Elaboration:

Discrepancies in the vulnerability repository may result when assets are acquired, modified, or retired but not reflected accurately in the asset inventory. To the extent that Vulnerability Analysis and Resolution process area activities result in inventory discrepancies, the organization’s overall ability to manage the operational resilience of high-value assets subject to vulnerability analysis and resolution is impeded.

5. Identify problems in the plan for performing and executing the process.

6. Take corrective action when requirements and objectives are not being satisfied, when issues are identified, or when progress differs significantly from the plan for performing the process.
7. Track corrective action to closure.

VAR:GG2.GP9 Objectively Evaluate Adherence

Objectively evaluate adherence of the vulnerability analysis and resolution process against its process description, standards, and procedures, and address non-compliance.

Elaboration:

These are examples of activities to be reviewed:

- alignment of stakeholder requirements and needs with the process scope, strategy, plans, and management strategies for specific vulnerabilities
- assignment of responsibility, accountability, and authority for process activities
- determining the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any
- verification of data confidentiality, integrity, and availability controls
- use of process data for improving strategies for protecting and sustaining assets and services

These are examples of work products to be reviewed:

- process plan and policies
- process scope and strategy, as well as strategies for managing specific vulnerabilities
- vulnerabilities that have been referred to the risk management process
- vulnerability data identification, analysis, recording, storage, remediation, monitoring, communication, protection, and distribution methods, techniques, and tools
- metrics for the process *(Refer to VAR:GG2.GP8 subpractice 2.)*
- contracts with external entities

VAR:GG2.GP10 Review Status with Higher Level Managers

Review the activities, status, and results of the vulnerability analysis and resolution process with higher level managers and resolve issues.

Refer to the Enterprise Focus process area for more information about providing sponsorship and oversight to the operational resilience management system.

VAR:GG3 Institutionalize a Defined Process

Vulnerability analysis and resolution is institutionalized as a defined process.

VAR:GG3.GP1 Establish a Defined Process

Establish and maintain the description of a defined vulnerability analysis and resolution process.

Establishing and tailoring process assets, including standard processes, are addressed in the Organizational Process Definition process area.

Establishing process needs and objectives and selecting, improving, and deploying process assets, including standard processes, are addressed in the Organizational Process Focus process area.

Subpractices

1. Select from the organization’s set of standard processes those processes that cover the vulnerability analysis and resolution process and best meet the needs of the organizational unit or line of business.
2. Establish the defined process by tailoring the selected processes according to the organization’s tailoring guidelines.
3. Ensure that the organization’s process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes.
4. Document the defined process and the records of the tailoring.
5. Revise the description of the defined process as necessary.

VAR:GG3.GP2 Collect Improvement Information

Collect vulnerability analysis and resolution work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization’s processes and process assets.

Elaboration:

These are examples of improvement work products and information:

- changes in operating conditions, risk conditions, and the risk environment that affect process results
- metrics and measurements of the viability of the process (Refer to VAR:GG2.GP8 subpractice 2.)
- lessons learned in post-event review of incidents and disruptions in continuity
- lessons learned that can be applied to improve operational resilience management performance
- the currency status of vulnerability data
- the confidentiality, integrity, and availability status of vulnerability data based on integrity and security tests
- reports on the effectiveness and weaknesses of controls
- process action plans and strategies that are not being satisfied and the risks associated with them
- resilience requirements that are not being satisfied or are being exceeded

Establishing the measurement repository and process asset library is addressed in the Organizational Process Definition process area. Updating the measurement repository and process asset library as part of process *improvement and deployment is addressed in the Organizational Process Focus process area.*

Subpractices

1. Store process and work product measures in the organization’s measurement repository.
2. Submit documentation for inclusion in the organization’s process asset library.
3. Document lessons learned from the process for inclusion in the organization’s process asset library.
4. Propose improvements to the organizational process assets.