**IT Risk Assessment Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the Risk Assessment Policy. This policy and procedure establishes the minimum requirements for the Risk Assessment Policy.

This policy is intended to meet the control requirements outlined in SEC520 and SEC501, Section 8.14 Risk Assessment Family, controls RA-1 through RA-5 as well as additional Commonwealth of Virginia controls.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all “YOUR AGENCY NAME” systems classified as sensitive.

# ACRONYMS

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

RA: Risk Assessment

SEC501: Information Security Standard 501

SEC520: Information Security Risk Management Standard 520

SSP: System Security Plan

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The Risk Assessment Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the risk assessment requirements as stipulated by the COV ITRM Security Standard SEC501, COV ITRM Risk Management Standard SEC520, and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all sensitive IT systems.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Roles** | IT Internal Audit Director | Agency Head | System Owner | System Admin | Information Security Officer |
| **Tasks** |  |  |  |  |  |
| Categorize and document information and information systems. | I |  | A/R |  | C |
| Include the system categorization in the ssp. | I |  | A/R |  | C |
| Review the security categorization on an annual basis. | I |  | A/R |  | C |
| Conduct and document assessment of risk. | I |  | A/R |  | C |
| Review and update risk assessment. | I |  | A/R |  | C |
| Create a risk finding. | I |  | A/R |  | C |
| Create a risk treatment plan | I |  | A/R |  | C |
| Submit a risk assessment plan and risk treatment plan to the ciso. | I | A |  |  | I |
| Receive reports from the risk register and verify implementation. | I | A |  |  | I |
| Verify and validate compliance. | A |  |  |  |  |
| Scan and analyze information systems and hosted applications for vulnerabilities. | I |  | A | R | R |
| Remediate vulnerabilities. | I |  | A | R | R |
| Review audit logs. | I |  | A | R | R |
| Document and report vulnerabilities and risks to ciso. | I | A |  |  | I |

# STATEMENT OF POLICY

In accordance with SEC520 and SEC501, PS-1 through PS-8, security categorization, risk assessments, and vulnerability scans shall be used for the execution, development and implementation of remediation programs at “YOUR AGENCY NAME”.

1. **SECURITY CATEGORIZATION** 
   1. The ISO shall require that:
      1. Information and the information systems must be categorized in accordance with Commonwealth policies and procedures;
         1. The authorization boundary is a prerequisite and must be clearly defined before beginning the security categorization.
         2. Security categorization describes the potential adverse impacts to “YOUR AGENCY NAME” operations, “YOUR AGENCY NAME” assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability.
      2. Security categorization results must be documented (including supporting rationale) in the system security plan (SSP) for the information system;
      3. The security categorization must be conducted as a “YOUR AGENCY NAME”-wide activity;
         1. Related staff, management, System Owner, and information security staff knowledgeable in the information created or collected by the program shall assist with the development of the security categorization.
      4. Security categorization must be part of the system development life cycle (SDLC);
         1. The security categorization must be reviewed and updated whenever there is a change in the information processed.
      5. The security categorization must be reviewed at least on an annual basis; and
      6. The security categorization decision must be reviewed and approved by the Agency Head or designated representative.
      7. Security categories must be used in conjunction with vulnerability and threat information in assessing the risk to an organization resulting from the operation of its information systems.
2. **RISK ASSESSMENT** 
   1. The ISO or designee must enforce the following Risk Assessment requirements for each IT system classified as sensitive to:
      1. Identify potential threats to the confidentiality, integrity, and availability of an IT system and the environment in which it operates;
      2. Determine the likelihood that threats will materialize;
      3. Identify and evaluate vulnerabilities; and
      4. Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.
   2. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and the Commonwealth based on the operation of the information system.
      1. Risk assessments also take into account risk posed to “YOUR AGENCY NAME” operations, “YOUR AGENCY NAME” assets, or individuals from external parties, including but not limited to:
         1. Service providers.
         2. Contractors operating information systems on behalf of the organization.
         3. Individuals accessing “YOUR AGENCY NAME” information systems.
         4. Outsourcing entities.
         5. Entities such as foreign nations and business competitors that may have an interested in information stored by “YOUR AGENCY NAME”.
      2. Risk assessments must be a collaborative effort among representatives of management, operational, technology and information security disciplines.
   3. The System Owner shall:
      1. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
      2. The RA shall be conducted as needed, but not less than once every three years.
      3. Document risk assessment results in a Risk Assessment Report, which includes, at a minimum, identification of all vulnerabilities discovered during the assessment, and an executive summary, including major findings and risk mitigation recommendations.
         1. Updated reports must be sent to the CISO.
      4. Review risk assessment results at least once a year to determine the continued validity of the RA;
      5. Update the risk assessment once a year or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system;
      6. Use the results of the “YOUR AGENCY NAME” BIA and of the Data Classification procedure as primary inputs to the RA;
      7. Create a risk finding for any risks identified in the risk assessment with a residual risk rating greater than a value of low; and
      8. Create a risk treatment plan for each risk assessment finding.
   4. The ISO or designee shall require that “YOUR AGENCY NAME” develop a risk assessment plan.
      1. The Agency Head shall submit the risk assessment plan to the CISO on an annual basis.
      2. The risk assessment plan must include the following:
         1. The agency name, agency abbreviation and agency number,
         2. The contact information of individual submitting the plan,
         3. The date of submission,
         4. The system full name and abbreviation,
         5. The planned assessor,
         6. The date the last risk assessment was conducted for the system, and
         7. Scheduled assessment completion date.

Note: Scheduled assessment completion date is the planned date of the completion of the future risk assessment covering a three year period from the submission date.

* 1. Until completion of all corrective actions in the risk assessment, the responsible Agency Head or designee shall receive reports, at least quarterly, from the risk register. The quarterly risk update will report progress toward implementing outstanding risk treatments.
  2. Upon completion of the risk treatments shown in the risk register, the responsible Agency Head or designee shall arrange for a follow-up review to verify implementation of the specified corrective actions.
  3. The Agency Head or designee shall submit to the CISO the following information:
     1. A record of all completed IT Risk Assessments conducted by or on behalf of the Agency.
     2. Agencies are required unless otherwise approved by the CISO to use the Risk Assessment Template found at: http://www.vita.virginia.gov/xxxx
     3. Each risk identified in the risk assessment template must contain:
     4. IT System Name
     5. Risk ID
     6. Sensitivity rating (e.g. Confidentiality, Integrity and availability)
     7. Date of risk assessment
     8. Risk vulnerability family (e.g. SEC 501 control)
     9. Vulnerabilities
     10. Threats
     11. Risk Summary
     12. Magnitude of impact (e.g. low, moderate, high, critical)
     13. Controls in place (brief description)
     14. For each risk identified, a Risk Treatment Plan must be submitted to the CISO and the plan shall include the:
     15. IT System affected
     16. Authoritative source (e.g. SEC 501, enterprise policy, operating instruction)
     17. Control ID (e.g. AC-1)
     18. Date risk identified
     19. Risk summary
     20. Risk rating (Low, Med-Low, Med, Med-High, High, Critical)
     21. Status
     22. Status Date
     23. Planned resolution;
     24. Resolution due date
     25. The Risk treatment plan for completed risk assessments must be submitted within 30 days of issuing the final risk assessment report. An updated risk treatment plan must be submitted quarterly (at the end of the quarter), until all resolutions are completed. All Risk Treatment Plans and quarterly updates submitted must have evidence of agency head approval.
  4. The “YOUR AGENCY NAME” IT Internal Audit Director is responsible for verifying and validating compliance with the provisions of this policy and procedure.

1. **VULNERABILITY SCANNING** 
   1. The ISO shall require that:
      1. Information system and hosted applications must be scanned for vulnerabilities at least once every 90-days for publicly facing systems and sensitive information systems and when new vulnerabilities potentially affecting the system/applications are identified and reported;
         1. The security categorization of the information system must guide the frequency and comprehensiveness of the vulnerability scans.
         2. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers).
         3. Vulnerability scanning must include scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms.
         4. “YOUR AGENCY NAME” shall considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.
         5. The following attributes, at a minimum, are required for vulnerability testing, as required by “YOUR AGENCY NAME”’s Commonwealth Security and Risk Management, and are necessary to evaluate compliance for security certification and best practice adherence:
            1. Device Name,
            2. IP address,
            3. Device Type,
            4. Wireless Access Points,
            5. Description,
            6. OS Platform,
            7. Primary Admin,
            8. Location,
            9. Service Type,
            10. Service Port,
            11. Service Port Type,
            12. Application,
            13. Users of Service,
            14. Network Name,
            15. Network Type,
            16. Location Type,
            17. Location Access,
            18. Owning Location,
            19. User Population Name and Type, and
            20. Primary User contact information (e.g. phone, email).
      2. Vulnerability scans must have defined a clear scope for all vulnerability scanning activities and designate knowledgeable and trained individuals to perform the scans. Prior to commencing vulnerability scanning efforts, the following should be addressed:
         1. Scanner selection – System Owners shall evaluate the tools for use within their respective environments.
            1. The network and host-based vulnerability scanner must provide the following capabilities:

Identify active hosts on networks.

Identify active and vulnerable services (ports) on hosts.

Identify vulnerabilities associated with discovered operating systems and applications.

* + - 1. Scope/boundaries – An active vulnerability scan must have a defined scope or boundary. The scan must be limited to a specific information system, system(s), subnet(s), or network(s) within the realm of responsibility for “YOUR AGENCY NAME”.
         1. Scans typically should be performed only on production systems and networks that are known to be stable and preferably during times of least impact to the critical functionality of the system. It is expected that vulnerability scanning will occur during various phases of the system’s life cycle.
      2. Coordination/announcement – Coordination with and/or notification to the relevant or affected parties, depending on the scope and purpose of the scans, must occur before an active vulnerability scan is performed, especially if that scan may result in a potential negative impact.
    1. The following must be addressed before and after the vulnerability scan:
       1. Update scanning software – Before the vulnerability scan is performed, the vulnerability scanner must be updated with the latest patches and database signatures/tests. Scanners that are not maintained and out of date will not contain the most recent signatures/tests and, as a result, vulnerabilities could be missed.
       2. Verify system availability – After completing the test, the System Owner shall check system status directly or by coordinating with the system administration team to ensure that the test did not result in unintended consequences and that the system remains operational.
    2. Vulnerability scanning tools and techniques must be employed that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
       1. Enumerating platforms, software flaws, and improper configurations;
       2. Formatting and making transparent, checklists and test procedures; and
       3. Measuring vulnerability impact;
    3. Vulnerability scan reports and results from security control assessments must be analyzed;
    4. Vulnerabilities must be remediated within 90 days in accordance with an organizational assessment of risk; and
    5. Information obtained from the vulnerability scanning process and security control assessments must be shared with designated personnel throughout the “YOUR AGENCY NAME” to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
    6. The ISO or designee shall enforce the following requirements:
    7. Vulnerability scanning tools must include the capability to readily update the list of information system vulnerabilities scanned.
    8. The list of information system vulnerabilities scanned must be updated at least once every 90 days or when new vulnerabilities are identified and reported.
    9. Vulnerability scanning procedures must be employed that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).
    10. Discerning what information about the information system is discoverable by adversaries must be attempted.
    11. Privileged access authorization must be included for selected vulnerability scanning activities to facilitate more thorough scanning.
    12. Historic audit logs must be reviewed to determine if a vulnerability identified in the information system has been previously exploited.
  1. The Agency Head shall document and report vulnerabilities and risks identified in the vulnerability scan and related remedial actions to CSRM once every 90 days.

Note: If no vulnerabilities were identified in a vulnerability scan, Agency must notify CISO that the vulnerability scan was conducted and there were no findings.

* + 1. Risks identified in Vulnerability scans must be reported to the CISO using the Risk Assessment and Risk Treatment Plan templates and include the following information:
    2. Date of Scan
    3. Host Name
    4. IP or DNS Entry
    5. Vulnerability description
    6. Severity level/Risk Rating (high, medium, low)
    7. CVE #
    8. Remediation action (e.g. what’s needed … disable port, etc.)
    9. Results of follow-up scan after remediation action is taken

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO” ““YOUR AGENCY NAME””)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

[ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

| Version History | | |
| --- | --- | --- |
| Version | Date | Change Summary |
| 1 | 09/28/2007 | Original document. Some was content taken from the superseded “YOUR AGENCY NAME” SEC Impact Analysis and Risk Assessment Procedure. |
| 2 | 02/01/2013 | Administrative Changes |
| 3 | 07/01/2014 | Complete rewrite of original document based on ITRM Information Security Standard Revision 8 with Role Matrix added. |
| 4 | 11/17/2021 | Formatting changes |