RABET-V Program Manual

Release 1.3

Center for Internet Security

Dec 24, 2025

INTRODUCTION

1 Introduction **1**
- 1.1 Program Goal . . . 1
- 1.2 Program Benefits . . . 1
- 1.3 Program Scope . . . 2

2 RABET-V Activities **3**

3 RABET-V Administrator **5**

4 RABET-V Activities **7**
- 4.1 RABET-V Iteration . . . 7
- 4.2 Timing Flexibility . . . 8
- 4.3 RABET-V Baselines . . . 8

5 Registered Technology Providers (RTPs) **9**
- 5.1 RTP Request Package . . . 9
- 5.2 Program Commitment . . . 9
- 5.3 Submission Types . . . 10
- 5.4 Submission Items . . . 10
- 5.5 Submission . . . 13
- 5.6 Product Listing . . . 14
- 5.7 Provider Deregistration and Product Delisting . . . 14
- 5.8 Deregistration Process . . . 14
- 5.9 Delisting Process . . . 15

6 Submission Review Process **17**
- 6.1 Inputs . . . 17
- 6.2 Outputs . . . 17
- 6.3 Workflow . . . 17

7 Organizational Assessment **21**
- 7.1 Organizational Assessment Methodology . . . 21
- 7.2 Organizational Maturity Rubric . . . 24
- 7.3 Organizational Baseline Scoring . . . 26

8 Architecture Assessment **29**

8.1 Architecture Assessment Methodology . . . 30
8.2 Architecture Maturity Rubric . . . 34
8.3 Rubric Configuration . . . 35
8.4 Architecture Baseline Scoring . . . 36

9 Test Plan Determination **39**
9.1 Inputs . . . 40
9.2 Outputs . . . 40
9.3 Workflow . . . 40

10 Product Verification **41**
10.1 Methodology . . . 41
10.2 Verification Methods . . . 42
10.3 Product Implementation Rubric . . . 43
10.4 Product Verification Baseline . . . 44

11 Reporting Process **49**
11.1 Inputs . . . 49
11.2 Outputs . . . 49
11.3 Workflow . . . 49
11.4 Report Statuses . . . 50
11.5 RABET-V Product Statuses . . . 50

12 Assessor Accreditation **53**

13 Eligibility **55**
13.1 Basic Eligibility . . . 55
13.2 Requirements for Maintaining Eligibility . . . 56
13.3 Preventing Conflicts of Interest and Impropriety . . . 56
13.4 Tailored Use Eligibility . . . 56
13.5 Curing of Lapses in Eligibility . . . 57

14 Organizational Competency **59**
14.1 Technical Capabilities . . . 60

15 Confidentiality and Work Products **63**

16 Application Process **65**

17 Quality Monitoring **67**

18 RABET-V Glossary **69**

19 RABET-V Control Families **73**
19.1 Security Control Families . . . 73
19.2 Accessibility Control Families. . . . 74
19.3 Usability Control Families . . . 74

20 Security Requirements **75**
20.1 1. Authentication Requirements . . . 75

20.2 2. Authorization Requirements 81
20.3 3. Boundary Protections Requirements 85
20.4 4. Data Confidentiality and Integrity Requirements 92
20.5 5. System Availability Requirements 100
20.6 6. Injection Prevention Requirements 103
20.7 7. Logging/Alerting Requirements 107
20.8 8. Secret Management Requirements 114
20.9 9. System Integrity Requirements 116
20.10 10. User Session Management Requirements 122

Index **125**

CHAPTER

ONE

INTRODUCTION

The Rapid Architecture-Based Enterprise Technology Verification (RABET-V) program is a rapid, reliable, and cost-effective approach to verifying enterprise systems. RABET-V is designed to introduce testing standards by which organizations can be assured of the security and reliability of the technology they use.

For more information of the background and motivation for RABET-V:

- `RABET-V Pilot 1 Report`
- `RABET-V Pilot 2 Report`
- `How to Improve Election Technology Verification White Paper`
- The EI-ISAC's Essential Guide to Election Security
- The Center for Internet Security's Security Best Practices for Non-Voting Election Technology Guide

1.1 Program Goal

The RABET-V program provides assurances of security, reliability, accessibility, and usability sufficient for technology providers and agencies to have confidence in their use in their environments. Organizations and their products are assessed on their capability to effectively build, test, monitor, and maintain their solutions through evidence-based assessment, automated tools, and product testing.

1.2 Program Benefits

Registered technology providers (RTPs) and agencies benefit from the RABET-V program in a number of ways. The RABET-V program:

- **Evaluates architectures** to assess the risk of changes. Understanding the architecture allows for streamlined testing for future versions, which saves time and money
- **Analyzes software development processes** to assess the likelihood of positive outcomes. Good software development processes reduce the risk that an organization will make a mistake in implementing a change
- **Prescribes different levels of testing** based on the type of change and the maturity of the product. Faster testing means a lower cost for technology providers

- **Re-evaluates new product versions** quickly for products with higher organizational and architecture maturity scores
- **Grounds all assessments in security best practices** listed in the security requirements appendix of this program manual. The 153 discrete RABET-V security requirements were constructed based on several national security standards.

1.3 Program Scope

RABET-V is intended for all technologies, excluding voting systems.

> **Note**
>
> A "voting system" is defined in the Help American Vote Act (H.R. 3295, Sec 301) as "(1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used—(A) to define ballots; (B) to cast and count votes; (C) to report or display election results; and (D) to maintain and produce any audit trail information; and (2) the practices and associated documentation used—(A) to identify system components and versions of such components; (B) to test the system during its development and maintenance; (C) to maintain records of system errors and defects; (D) to determine specific system changes to be made to a system after the initial qualification of the system; and (E) to make available any materials to the voter (such as notices, instructions, forms, or paper ballots)."

CHAPTER

TWO

RABET-V ACTIVITIES

RABET-V consists of three core *activities*, each performed by an *accredited assessor organization*:

1. *Organizational Assessment*: measures the quality of a technology provider's product development practices to answer the question "how good is the organization at developing technology products?"
2. *Architecture Assessment*: examines the product's components and environment at both the system and software levels to develop a picture of risk and risk mitigation to answer the question "how well-designed is the architecture underlying the product?"
3. *Product Verification*: confirms the ability of the system to prevent unintended actions or output to answer the question "does the product prevent unintended outcomes?"

These activities result in a set of maturity scores that are used to assess the risk of changes in a particular *product*. Understanding the *organizational maturity*, *architecture maturity*, and *product implementation scores* allows the *RABET-V administrator* to prescribe different levels of testing for product revisions. Certain types of changes to a product with higher organizational and architecture maturity scores can be evaluated more quickly in subsequent iterations.

Through RABET-V, registered technology providers get more feedback and a roadmap for improvement. Agencies can request more detailed reporting of a technology provider's security, reliability, accessibility, and usability and evaluate the organizational maturity of an organization when considering technology products. Both technology providers and agencies alike get a more efficient verification process.

CHAPTER

THREE

RABET-V ADMINISTRATOR

The *RABET-V administrator* is a central body responsible for overseeing the RABET-V program, including:

- Accepting requests from and managing the list of RABET-V registered technology providers
- Accepting requests from and managing the list of accredited assessor organizations
- Hosting and managing content and workflows on the RABET-V portal, a platform for accredited assessor organizations and RTPs to register for the RABET-V program and communicate about RABET-V activities
- Managing the RABET-V program content and manuals, making changes as necessary and as supported by the *strategic advisory committee*

  RABET-V is a trademark of The Center for Internet Security Inc. The Turnout serves as the RABET-V administrator.

CHAPTER

FOUR

RABET-V ACTIVITIES

The RABET-V program consists of seven discrete activities from *registered technology provider (RTP)* registration to reporting. Each *activity* may be scaled or eliminated based on risks attributed to the product changes and the maturity scores from the previous submission. Risk decisions are informed by the product's *organizational maturity score*, *architecture maturity score*, and *product implementation score*. Each time the RABET-V process is initiated, it is called a *RABET-V iteration*.

4.1 RABET-V Iteration

Throughout the process, assessment activities produce scores that are shared with the RTP after the activity is complete. All scores are tentative until the entire RABET-V process is complete. Each activity draws heavily on the RABET-V security requirements.

1. **RTP Registration:** The RTP submits documentation to begin the RABET-V iteration. This submission contains information from the RTP on both its organization and the product under review
2. **Submission Review:** The *RABET-V administrator* reviews the submission for completeness, determines which activities are necessary for the submission type, and assigns assessors to perform the necessary activities
3. **Organizational Assessment:** An *accredited assessor organization* reviews the RTP's approach to developing software to determine its maturity, which will be used throughout the RABET-V process and subsequent submissions by the RTP. A demonstrably high level of maturity can reduce the burden of review across all activities. One can think of this as assessing the general trustworthiness of an RTP to reliably implement any given product feature or capability. A tentative score is provided to the RTP upon completion of the activity
4. **Architecture Assessment:** An accredited assessor organization reviews the product's architectural approach to determine its maturity with regard to various services. A demonstrably high level of maturity can reduce the burden of review for a specific change. One can think of this as assessing the trustworthiness of the product that changes to one product feature or service will not have unintended implications for other aspects of the product. A tentative score is provided to the RTP upon completion of the activity
5. **Test Plan Determination:** The RABET-V administrator produces a test plan based on the outputs from the organizational assessment and the architecture assessment

6. **Product Verification:** An accredited assessor organization executes the test plan and produces product verification scores
7. **Reporting:** The RABET-V administrator produces detailed reports for RTPs and a statement of the verification status

4.2 Timing Flexibility

While these activities are presented in a common order, there is flexibility in the timing of the organizational and architecture assessments. For instance:

- If an organization has a consistent development process across all of its products and business units, an RTP can complete an organizational assessment before submitting a specific product. The RABET-V administrator encourages this as it can speed the initial *iteration* for a product
- Similarly, if an RTP has a significant process change, it can request a new organizational assessment at any time. This can impact the scores, and thus test scaling, of that RTP's products
- The organizational assessment and architecture assessment activities share some information between each other, but are largely independent and can often occur in parallel

4.3 RABET-V Baselines

RABET-V uses baseline scoring in organizational, architecture, and product verification to determine whether a product is verified. The baselines in each activity must meet a minimum score and a specific set of requirements. The table below contains the existing miminum score baselines, links to the baselines in each activity that define the additional requirements, and the comparison to past versions.

Table 1: RABET-V baselines comparison

RABET-V Activity	2023 Baseline	2024 Baseline	2025 Baseline(Current)
Organizational	1.20	1.20	1.20
Architecture	1.50	1.50	1.50
Product Verification	2.00	2.00	2.00

CHAPTER

FIVE

REGISTERED TECHNOLOGY PROVIDERS (RTPS)

A *registered technology provider (RTP)* is an organization that develops enterprise technology and has met the minimum requirements in this section.

5.1 RTP Request Package

Technology providers register for the RABET-V program by submitting a completed request package to become an RTP. A complete package will contain the following information:

- Company name and legal address
- Sales and technical support points of contact
- Website URL
- Company description

To complete the request package, please follow this link to the RABET-V registration portal.

5.2 Program Commitment

RTPs must agree to the RABET-V program commitment. The commitment establishes the ethical and responsible behavior expected by all program providers.

The program commitment requires:

- Accurate representation of the product capabilities and its security provisions to RABET-V administrators, customers, and other stakeholders
- Organization implementation and regular assessment against an organizational security framework like the CIS Controls. The RTP must provide evidence of regular audits (e.g., audit letters, reports) to the *RABET-V administrator*
- Continuous product maintenance, including patching components within reasonable time frames

5.3 Submission Types

The RABET-V process begins with a product submission from an RTP. All product submissions are either an *initial product submission* or a *product revision submission*.

5.3.1 Initial Product Submission

The initial product submission is a first-time submission of a product to the RABET-V process. It includes statements about the product and the RTP that will be used throughout the RABET-V process. An initial product submission is required for each unique product an RTP would market and sell independently. An RTP may be required to submit a new initial product submission if more than three years have elapsed since they last submitted a product revision submission.

5.3.2 Product Revision Submission

A product revision submission is for changes being made to a product that has already been through the RABET-V process. It includes information about changes to the product since the last submission.

An RTP can make a product revision submission at any time after that product has been verified through an initial *RABET-V iteration*. It can improve the likelihood of a smooth process by engaging the RABET-V administrator ahead of the submission about upcoming changes and understanding how the established *test plan* will be impacted by deviations from the previous version.

A product revision submission requires only the version change list, artifacts, desired deployment date, and version numbers, as well as any other meaningful changes, such as to the organizational process.

5.4 Submission Items

This section describes submission artifacts for the RABET-V process. Each description indicates if it is required for an initial product submission, product revision submission, or both.

5.4.1 Product Goals

The product goals statement is a description of the product's purpose in non-technical language. It should be brief: a one or two paragraph summary of what the product is designed to do. The RTP can update the product goals during any product revision submission and should always confirm whether there have been any changes.

This description will be used by the RABET-V administrator in the submission review activity to determine if the stated security claims align with the product goals. For example, if the product goals include managing sensitive voter information, the RABET-V administrator will expect to see security claims designed to protect sensitive voter information.

Initial Product Submission: Always required

Product Revision Submission: When changed from last submission

5.4.2 Expected Usage

The expected usage statement describes how the RTP expects the agency to use the product. While it can communicate this through a number of means, a good approach is through high-level use cases that list the actions and interactions between involved parties and the system to achieve the product goals. Usage of the product will be limited to the use cases expressed in the expected usage. The RTP can update the expected usage during any revision submission and should always confirm whether there have been any changes.

Initial Product Submission: Always required

Product Revision Submission: When changed from last submission

5.4.3 Product Claims

The product claims workbook is a listing of requirements met by the product. This workbook is a product of the *security requirements* in the appendix of this program manual. The RTP completes and maintains this workbook for any submitted product.

For each requirement, the RTP will describe the implementation approach and whether the requirement is "Met," "Partially Met," "Not Met," or "Not Applicable." If the RTP only implements the requirement on certain components, it should provide details and the rationale for excluding it from other components. The RTP should include well-reasoned arguments for the implementation decisions and how they result in the appropriate level of security for the product. This approach allows each product to implement a unique approach to the application that is specific to its goals and usage. To ensure proper testing to meet or exceed the benchmark, the claims should cover the minimum controls to pass the benchmark. For example the 2023 benchmark states that 100% of Level 1 controls must pass and 50% of the Level 2 and 3 controls must pass.

The RTP can update the product claims during any product revision submission and should always confirm whether there have been any changes.

Initial Product Submission: Always required

Product Revision Submission: When changed from last submission

5.4.4 Process Descriptions

RTP's should submit documentation related to the RTP's development processes and operating environment. These should cover key aspects of software development as described in the OWASP Software Assurance Maturity Model (SAMM), which is used as the foundation for the *organizational assessment*.

The type of documentation requested includes:

1. Policy and compliance documents that are related to or help define efforts related to acquiring, managing, designing, developing, testing, and supporting software at the organization
2. Process related documents that help define which processes the RTP follows related to software activities

3. A representative sample of artifacts from completed activities related to the above policy and compliance or process related activities

Initial Product Submission: Preferred, but not required

Product Revision Submission: When changed from last submission and in cases when a new product is being submitted with a different business unit, development team, or development process

5.4.5 Architecture Documentation, Diagrams, and Related Representations

The architecture documentation and diagrams is a set of documents that fully describe the architectural design of the product. The product's architecture can be described using diagrams, narrative, or, ideally, a combination of the two.

The RTP should submit documentation of the architecture at the system and the software levels. The system architecture should describe deployable subsystems, such as web services, databases, as well as hardware components such as firewalls and tablets. The software architecture should be described in terms of software components.

The *term* component is used generically within RABET-V to describe part of a product. Components can be broken down into subcomponents, as required. The architecture should be deconstructed to the level that exposed functionality (e.g., a particular web service, program API) can be identified.

RABET-V does not dictate a particular notation for submitted diagrams; however, where possible RTP's should follow provided examples, which are based on UML component diagrams.

RABET-V uses automated analysis tools to evaluate software architecture without direct access to source code. RTPs will be required to process their source code through such tools in order to make further software level analysis possible.

Initial Product Submission: Preferred, but not required

Product Revision Submission: When changed from last submission

5.4.6 Product Environment and User Documentation

The RTP must provide access to a product environment that can be used by the administrator to conduct the RABET-V iteration. This should be a dedicated environment running the new product version. The administrator must provision user accounts and test data consistent with the expected usage statement. Test data should not include sensitive information, but may include data that is sanitized as necessary to remove personal information, product passwords, etc.

On the initial product submission, the RTP should include user documentation and be available for a meeting to assist the administrator in understanding the product usage. Updated documentation should be provided when changes are significant enough to warrant the update. User documentation must include the product version number it was written to support.

For many products, the product environment is the deployment of the web application to a sandbox hosting environment. For products like electronic pollbooks with physical devices, the product environment must include deployments of the product revision on physical devices provided to the administrator.

Initial Product Submission: Always required

Product Revision Submission: Always required

5.4.7 Summary of Revision Submission Artifacts

The RTP can submit a *product revision* to the RABET-V process at any time. Engaging the administrator about upcoming changes and consulting the existing Test Plan will help the RTP better prepare their submission.

All revision submissions require the following artifacts:

1. Change list - Indicates which components have changed and what level of change was made. It should reference the components identified in the architecture assessment activity
2. Artifacts - The product development artifacts identified in the existing organizational review. These artifacts provide the necessary information on product changes to conduct a review of the changes in the change list
3. Desired Deployment Date - Target date for deploying the product revision in a production environment
4. Version Number - The version number of the current product revision. It must indicate and correspond to code branches and change size (i.e. minor version number changes must correspond to minor changes)

A provider may change any of the initial product submission items during a product revision submission by providing updated information and alerting the administrator. If they are not submitting updates for any given artifact, the RTP will have to attest to there being no change.

Initial Product Submission: Not applicable

Product Revision Submission: Always required

5.5 Submission

Once the initial product submission or product revision submission package is complete, it should be submitted electronically to the RABET-V Administrator through the RABET-V Portal.

Items	Initial Product Submission	Product Revision Submission
Product Goals	Always required	When changed from last submission
Product Claims	Always required	When changed from last submission
Process Descriptions	Preferred, but not required	When changed from last submission
Architecture Documentation & Diagrams	Preferred, but not required	When changed from last submission
Product Environment & User Documentation	Always required	Always required
Summary of Revision Submission Artifacts	Not applicable	Always required

5.6 Product Listing

After going through the RABET-V Program, RTPs may choose to list one or more of their products on the *RABET-V public listing site* as a listed product. RABET-V listings include the following information:

- Company name
- Product name
- Product description, including version and configuration details
- Verification status
- RABET-V verification baseline met
- Date of verification

5.7 Provider Deregistration and Product Delisting

Failure to meet the requirements of the program commitment can lead to deregistration of the RTP and delisting of the RTP's products. Activities subject to deregistration are any that breach the program commitment or other activities that undermine the intent of the RABET-V program.

5.8 Deregistration Process

The RTP will be notified of the reason for deregistration and given 60 days to remedy. If the breach of program commitment has not been remedied within 60 days, the RTP will be deregistered.

5.9 Delisting Process

If a product has not been resubmitted to the RABET-V program in the last three years, the product will be delisted. The RTP will be notified of a delisting action with 90 days notice.

Products may also be delisted if a substantial issue, such as discovery of a critical vulnerability, becomes known. Generally, the RTP will receive a cure notice and will be delisted 60 days after the notice.

In the event of a severe issue, the RABET-V administrator reserves the right to delisted the product immediately and until the issue has been resolved.

CHAPTER

SIX

SUBMISSION REVIEW PROCESS

Once the *RTP* has made a submission, the *RABET-V administrator* will review the submitted information, determine which *RABET-V activities* are necessary for this *iteration*, and assign an {term}`accredited assessor organization ' for each activity.

6.1 Inputs

- The RTP's submission package
- The RTP's *organizational assessment*, if applicable
- Prior reviews, if applicable

6.2 Outputs

- Submission review checklist indicating submission type, change type (for a product revision submission), and which RABET-V activities should be performed in this iteration

6.3 Workflow

6.3.1 Review package for completion

See *RTP submission* for submission requirements.

Initial product submission

All RABET-V activities are required. Ensure all items on the submission review checklist are included in the submission. For each step, indicate on the submission review checklist if the respective item is present or missing.

Product revision submission

Some RABET-V activities may not be required. Complete the remainder of the steps in this process to determine which activities are required for this submission. For each step, indicate on the submission review checklist if the respective item is present, missing, or not required.

6.3.2 Validate Claims

The submitted control claims must cover the minimum benchmark for controls to be testable. If the claims do not cover the minimum number of controls, the RTP will need to update the claims submission to cover the minimum benchmark.

6.3.3 Validate change list

The approach to validating the change list will vary based on the findings for the *change list artifact* in the previous organizational assessment:

1. Reliable: change list validation can be skipped or limited to high-level spot checking
2. Otherwise: validate the change list by manual or automated means

Record the result in the submission review checklist.

6.3.4 Determine change type

(For product revision submissions only)

Given the validated change list, determine which change types apply to the revision. Change types are listed below:

Change Type Number	Change Type Description
1	Other major or multiple change(s) to in-scope services
2	Source code change to in-scope services
3	Major configuration change to in-scope services
4	Security patch of in-scope services
5	Dependency updates for in-scope services
6	Minor configuration change to in-scope services
7	Source code change interfacing in-scope services
8	Source code change unrelated to in-scope services
9	3rd party software patch to in-scope services
10	Operating system patch
11	Other software or configuration change

6.3.5 Determine if the organizational assessment is necessary

The organizational assessment is required when one of the following conditions is true:

1. The submission is an initial product submission
2. The RTP has requested a new organizational assessment in order to update organizational maturity scores
3. It has been more than 3 years since the last organizational assessment was performed
4. Artifacts provided by the RTP indicate a significant process change has occurred

Record the result in the submission review checklist.

6.3.6 Determine if the architecture assessment is necessary

The architecture assessment is required when one of the following conditions is true:

1. The submission is an initial product submission
2. The RTP has requested a new architecture assessment in order to to update the architecture maturity scores
3. The change list indicates the addition, removal, or modification of major architecture components since the last architecture assessment

Record the result in the submission review checklist.

6.3.7 Assign Accredited Assessor Organizations

The RABET-V administrator will assign accredited assessor organizations to perform the required RABET-V activities.

CHAPTER

SEVEN

ORGANIZATIONAL ASSESSMENT

The organizational assessment measures the quality of a *registered technology provider's (RTP)* product development practices to answer the question "how good is the organization at developing technology products?".

It provides *organizational maturity scores* for the RTP. It uses OWASP's Software Assurance Maturity Model (SAMM) as the basis for its evaluation, expanding the SAMM model to include practices and activities for a human factors area that include usability and accessibility. Thus, the six areas in the organizational assessment are:

- Governance
- Design
- Implementation
- Verification
- Operations
- Human Factors

In addition to providing the maturity scores, the organizational assessment determines the reliability of RTP-generated artifacts that can be used by RABET-V. By using reliable RTP-generated artifacts, the RABET-V process will not have to reproduce these artifacts (i.e., test results).

The organizational maturity scores and reliability of RTP-generated artifacts are used to help determine the types of testing conducted by RABET-V for product revisions. The organizational maturity scores are combined with the *architecture maturity scores* to support risk based testing in the *product verification step*.

7.1 Organizational Assessment Methodology

For more information about what is expected for the organizational assessment, see the *provider submission* activity and the *RABET-V security requirements*.

7.1.1 Inputs

- Process descriptions
- Interviews with RTP

7.1.2 Outputs

- Organizational maturity scores
- List of product development artifacts usable for verification
- High level executive summary of the process, findings, organizational maturity score, and tailored recommendations
- Completed organizational assessment toolbox

7.1.3 Workflow

Review Existing Documentation

An accredited assessor reviews existing documentation submitted by RTPs, including:

1. Policy and compliance documents that are related to or help define efforts related to acquiring, managing, designing, developing, testing, and supporting software at the organization
2. Process related documents that help define which processes the RTP follows related to software activities
3. A representative sample of artifacts from completed activities related to the above policy and compliance or process related activities

Discussion Sessions

An accredited assessor leads discussions with the different roles supporting the efforts related to the RTP's software development process. The discussions will last approximately 60-90 minutes. Sessions are driven by the organizational maturity rubric and are not checklist-based, but discussions on how processes and procedures are implemented and conducted throughout the organization.

Below are some of the common organizational roles held by individuals that would be interviewed:

1. Application/software security lead or equivalent party with responsibilities for defining and managing the integration of security into software
2. Business analyst or similar role with responsibilities related to requirements, user stories, etc.
3. Project manager or similar role with responsibilities for guiding teams through the processes to develop, acquire, and maintain software
4. Application architect or similar role with responsibilities to ensure good design and architecture for applications

5. Developer or similar role that has responsibilities to write code and some testing
6. Quality assurance/tester or similar role that handles the primary testing for software or applications
7. DevOps engineer or similar role with responsibilities related to build and deployment processes for software
8. Incident response/support or similar roles with responsibilities for helping support, triage, respond to issues in production systems

Determine Artifact Reliability

RABET-V can expedite product verification if certain software development artifacts are found to be reliable. When artifacts are found to be reliable, the RABET-V process may use them instead of reproducing similar artifacts and tests. However, this does not mean RABET-V must use them. The RABET-V process may include reproducing the results submitted by the RTP in order to validate the artifacts are reliable.

The organizational assessment is used to help determine if the following artifacts are accurate and consistently available for *RABET-V iterations*. If the RTP has additional software development artifacts that it believes are reliable and beneficial to streamlining the RABET-V process, it may request those artifacts to be evaluated and the test plan updated to account for the artifacts.

Change List

The change list is the most important software development artifact used by RABET-V when performing product verification in a revision iteration. It is critical that the list is accurate, detailed, and complete. While RTPs can submit manually generated change lists, they may take longer to process than automated change lists built from the central source code repository and reviewed by system architects and product owners.

During the organizational assessment, the method used for building change lists will be discovered and sample change lists will be reviewed for accuracy and completeness. If the change list is determined to be reliable, the RABET-V process will use the RTP's change list and not generate its own. If the change list is not reliable, the RABET-V process will explore other ways to produce an accurate change list, which may take additional time and resources.

Automated Configuration Assessments

Security configurations are a major part of ensuring that systems contain properly implementing security controls. Using configuration guidance, such as the CIS Benchmarks, leads to consistent security outcomes. Automated configuration assessment tools, such as the CIS configuration assessment tool (CIS-CAT), can ensure guidance is being followed for every release.

During the organizational assessment, the assessor will determine if the RTP is subscribed to configuration guidance and if they are using a reliable assessment tool. If so, the results of the assessment tool will be used during RABET-V iterations to verify certain requirements. If this artifact is not present or reliable, the product verification activity will have to perform additional testing to verify secure configurations.

Automated Vulnerability Assessments

Automated vulnerability assessments check system components for known vulnerabilities. These assessments primarily check third party components for known vulnerable versions of software. If deemed appropriate by the organizational assessor and the Administrator, RTPs that are regularly performing automated vulnerability scans on the product networks and software will have their results used during the Product Verification activity in lieu of RABET-V reviewer performing new scans. During the organizational assessment, reviewers will investigate the scope, frequency, and tooling used by the technology provider to determine if there is sufficient coverage and accuracy.

Automated Unit Testing

Automated unit testing is a way to regression test large and complex applications efficiently. It takes significant investment on the part of the RTP to build test suites that are robust and accurate. For RTPs that have invested in this capability, the results of their internal testing can be used to partially offset RABET-V product verification. The organizational assessment will look at the coverage and depth of the current automated testing routines, as well as the RTP's commitment to maintaining its test suites.

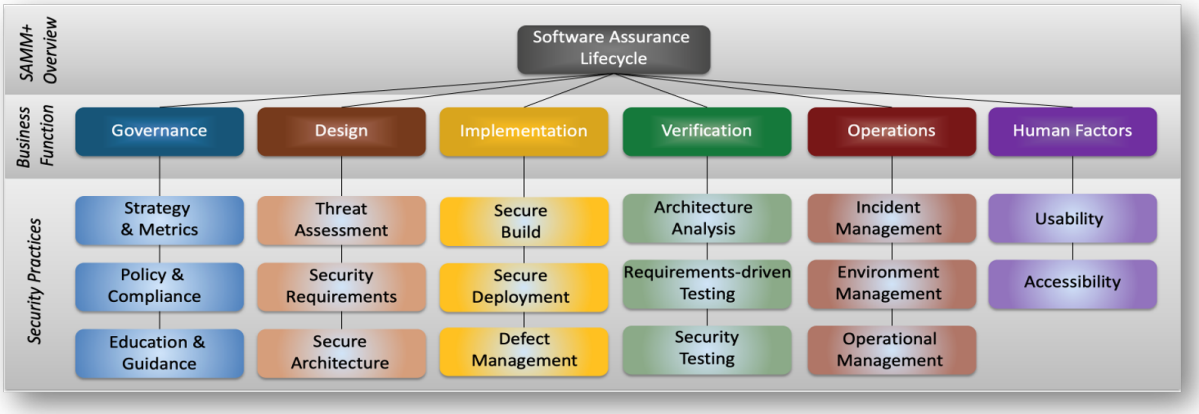
Third Party Security Analysis

RABET-V strongly encourages RTPs to receive regular, in-depth security audits on their systems. For example, there are audits that focus on hosting security and application security. These audits, if performed against a reliable standard and performed recently, can be used in RABET-V in lieu of repeating similar evaluations.

7.2 Organizational Maturity Rubric

The organizational assessment measures the maturity of the RTP's software development processes for security and usability. It results in an organizational maturity score, that is based on the OWASP Software Assurance Maturity Model (SAMM).

Maturity scores are provided for each of the 17 software development areas (15 SAMM plus usability and accessibility). The scores range from zero to three, where three is the best.



As with each of the assessment modules, the Organizational Assesment has a baseline defined that will determine whether or product will be Verified or not by the RABET-V process. The baseline is a combination of minimum scores for a subset of questions, and an overall maturity score that needs to be met or exceeded.

7.2.1 Accessibility

Accessibility is often overlooked as a development priority. It may be hard for developers without a disability to conceptualize needing or using accessibility features, but it's easy to find examples that may be possible for anyone to imagine. For example, some software developers developed repetitive stress injuries and turned to speech-to-text aids to continue working in their profession. Beyond the general necessity, adhering to accessibility standards is often a hard requirement for software solutions in many state systems.

Accessibility Maturity Levels	Quality Criteria	Required Activity
Level 0		
Level 1: Automated conformance to accessibility guidelines	Performs automated accessibility validation during development.	Use automated testing tools during development for: All major releases (partial credit)All significant changes to user interface functionality (full credit)Other (no credit)
Level 2: Testing with accessibility tools	Perform accessibility tests with commercial accessibility software and OS-specific features, including using personas and scenarios	Use commercial software, OS-specific features, and personas and scenarios for:All major releases (partial credit)All significant changes to user interface functionality (full credit)Other (no credit)
Level 3: Formal accessibility testing and analysis program	Use of research methods and experts to test prototypes with users that have accessibility needs.	Conduct accessibility testing and integrate results for: All major releases (partial credit)All significant changes to user interface functionality (full credit)Other (no credit)

7.2.2 Usability

Usability testing and analysis helps bridge the gap between a solution that meets a set of requirements and a solution that meets the needs of the organization, people, and processes. Meeting usability objectives is the distinction between a solution that people want to use (i.e., meets a set of requirements and usability needs) versus one they don't (i.e., solely meets a set of requirements).

Users will attempt to reduce friction in completing their desired task. A poorly designed user experience will result in users finding workarounds, often circumventing well-intentioned

security controls. For a product to achieve the risk mitigation intended by its requirements, it must integrate usability principles with security controls and, thus, an organization's maturity in implementing usability is critical to its security outcomes.

Usability Maturity Levels	Quality Criteria	Required Activity
Level 0		
Level 1: Formally established feedback loops with customers	Established processes for receiving feedback from customers and incorporating that feedback into the product	Incorporation of feedback into products for: All major releases (partial credit)All updates involving user-facing functionality (full credit)Other(no credit)
Level 2: Deploy enhanced feedback capabilities	Interview users, accept feedback directly through the product, collect logs and analytics through the product, or other similar approaches; from these, product form reports on findings and plans for incorporating feedback	Use commercial software, OS-specific features, and personas and scenarios for: Most major releases (partial credit)All significant changes to user interface functionality (full credit)Other (no credit)
Level 3: Formal usability testing and analysis program	Formal research on the business processes and users' behaviors, and conduct usability studies with users interacting with a prototype or version of the software solution.	Conduct formal usability testing and integrate results for: Most major releases (partial credit)All significant changes to user interface functionality (full credit)Other (no credit)

7.3 Organizational Baseline Scoring

The organizational baseline score is a combination of two elements: a minimum score for each question in a specific subset that are deemed critical, and an overall maturity score.

The minimum required overall organizational maturity score to meet the baseline for verification is 1.20.

The tables below outline the critical subset of questions and the minimum required score in each to contribute to the baseline score. A sufficient score in the remaining questions to get to an overall maturity score is also needed to meet the organizational baseline.

Business Function	Question	Baseline Score
Governanc	Do you understand the enterprise-wide risk appetite for your applications?	0.50
Governanc	Do you have and apply a common set of policies and standards throughout your organization?	1.00
Governanc	Do you have a complete picture of your external compliance obligations?	1.00
Governanc	Do you have a standard set of security requirements and verification procedures addressing the organization's external compliance obligations?	0.50
Governanc	Have you identified a security champion for each development team?	0.50

Business Function	Question	Baseline Score
Design	Do you identify and manage architectural design flaws with threat modeling?	0.50
Design	Do project teams specify security requirements during development?	0.50
Design	Do teams use security principles during design?	0.50
Design	Do you evaluate the security quality of important technologies used for development?	0.50
Design	Do you have a list of recommended technologies for the organization?	0.50
Design	Do you enforce the use of recommended technologies within the organization?	0.50

Business Function	Question	Baseline Score
Implementatior	Is your full build process formally described?	0.50
Implementatior	Do you have solid knowledge about dependencies you're relying on?	0.50
Implementatior	Do you handle third party dependency risk by a formal process?	0.25
Implementatior	Do you use repeatable deployment processes?	1.00
Implementatior	Do you consistently validate the integrity of deployed artifacts?	0.25
Implementatior	Do you limit access to application secrets according to the least privilege principle?	0.50
Implementatior	Do you track all known security defects in accessible locations?	1.00

Business Function	Question	Baseline Score
Verification	Do you review the application architecture for mitigations of typical threats on an ad-hoc basis?	0.25
Verification	Do you test applications for the correct functioning of standard security controls?	0.50
Verification	Do you consistently write and execute test scripts to verify the functionality of security requirements?	0.25
Verification	Do you scan applications with automated security testing tools?	0.50
Verification	Do you customize the automated security tools to your applications and technology stacks?	0.25
Verification	Do you manually review the security quality of selected high-risk components?	0.50
Verification	Do you understand the enterprise-wide risk appetite for your applications?	0.50

Business Function	Question	Baseline Score
Operations	Do you analyze log data for security incidents periodically?	0.50
Operations	Do you follow a documented process for incident detection?	1.00
Operations	Do you respond to detected incidents?	1.00
Operations	Do you use a repeatable process for incident handling?	0.50
Operations	Do you have a dedicated incident response team available?	0.25
Operations	Do you harden configurations for key components of your technology stacks?	0.50
Operations	Do you have hardening baselines for your components?	0.50
Operations	Do you identify and patch vulnerable components?	1.00
Operations	Do you follow an established process for updating components of your technology stacks?	0.50
Operations	Do you protect and handle information according to protection requirements for data stored and processed on each application?	1.00

Business Function	Question	Baseline Score
Human Factors	Do you have a formal feedback loop with your customers?	1.00
Human Factors	Do you perform automated accessibility validation during development?	1.00

CHAPTER

EIGHT

ARCHITECTURE ASSESSMENT

The architecture assessment examines the product's *components* at both the system and software levels to develop a picture of risk and risk mitigation to answer the question "how well-designed is the architecture underlying the product?".

The architecture assessment is designed to evaluate the product's architectural support for the *RABET-V security control families*. This evaluation produces an *architecture maturity score* for each security control family and identifies the components that provide each *security service*. This score does not measure how well the *product* executes the security service (i.e., its implementation score), just how mature the architecture is that supports each security service.

Note

At this time, the architecture assessment only reviews security services; when there are non-security control families implemented in the RABET-V process, this will be revisited.

The architecture maturity scores and component mappings are used to help assess the risk that changes to the product will negatively impact the security services. These are used in the *test plan determination* to identify how to test the product changes. Higher architecture maturity scores, in conjunction with organizational maturity scores, may indicate that less testing is needed to validate that changes have not created increased risk in the product.

The architecture assessment identifies the product *components* at the system and software levels that expose functionality, and the security services that *protect* those functions. Security service components are classified as `composite` or `transparent`. A *composite security service* component requires some level of implementation in the software (e.g., encryption or input validation). A *transparent security service* component requires no integration with the software; examples include firewall, transparent disk encryption, and physical security.

This activity also addresses the system and software architecture viewpoints. The system level diagram(s) identify the larger components of the environment used to host and manage the software application(s). The software level diagrams identify the components a layer deeper into the software application(s).

The architecture assessment will result in a score for each of the control families and an overall score. To achieve a verified status in the architecture assessment, an architecture would need to score high enough to meet or exceed the baseline score defined for each security control family and the overall score.

8.1 Architecture Assessment Methodology

For more information about what is expected for the architecture assessment, see the *provider submission* activity and the *RABET-V security requirements*.

8.1.1 Inputs

- The RTP processes their source code through designated application security and software architecture analysis tools: Mend and Lattix. For more information about what is expected for the architecture diagrams and description, see the *Provider Submission* activity
- The *security control families* provide guidance as to the needed controls to help protect the product and related data
- The architecture maturity rubric was created to help score the product architecture in the categories of reliability, manageability and consistency, maintainability (comprised of modularity and isolation), and depth of control coverage (i.e., defense-in-depth)
- The staff of the RTP will be interviewed during several tasks, including the system and software architecture assessment
- Inputs provided by the output of prior tasks are described in the narrative below

8.1.2 Outputs

- **Architecture maturity workbook** containing an executive summary tab, system level diagram(s), and architecture scoring
- **Architecture maturity scores** based on the maturity scoring rubric: architecture is assigned scores at various levels for each security control family which corresponds to how well it supports the mitigations within that family. These scores are calculated at five layers, starting at the most detailed level of security service implementation per component or interface and rolling up to result in a master architecture score
- **Interstitial outputs** between tasks are described in the narrative below

8.1.3 Workflow

Tasks

Perform System Architecture Assessment

The system level assessment takes the provider-submitted architectural documentation as input, along with interview sessions with individuals who possess knowledge about the system and software architecture. The security services the application provides are enumerated using the threat modeling methodology.

Outputs:

- Security Service Listing
- System Architecture Diagrams
- System Level Scores (including depth)

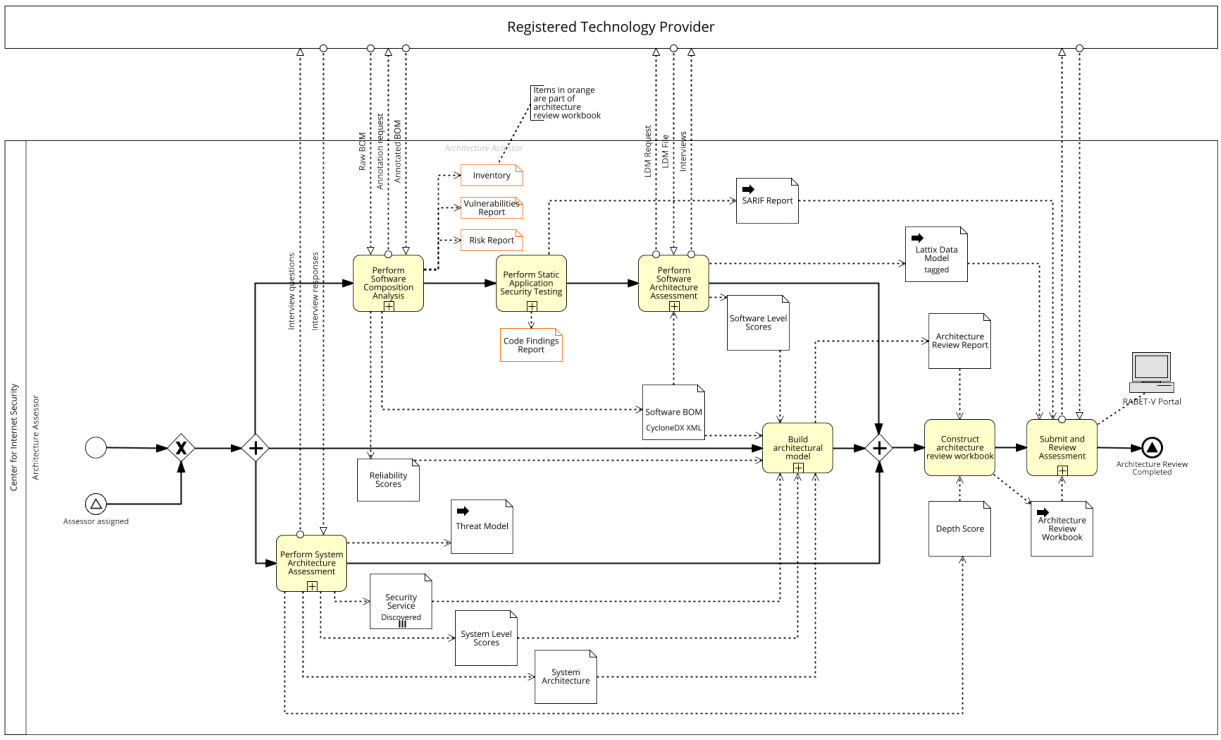


Fig. 1: A *BPMN* process model of the architecture review process

- Threat Model

Perform Software Composition Analysis

Software composition analysis examines the third-party libraries used by the product, including licenses, maintainers, and known vulnerabilities. RTPs submit a Software Bill of Materials (SBOM) in an approved format for analysis against vulnerability databases. This task produces reliability scores for some security services.

Outputs:

- Reliability Scores
- Software BOM
- Vunerabilities Report

Perform Static Application Security Testing

Perform automated Static Application Security Testing using Mend. This step does not affect scoring, but is instead used provided to pentesters to gain targeted insights into potential weaknesses.

Outputs:

- SARIF Report

Perform Software Architecture Assessment

Accredited assessor organizations analyze the software architecture using architectural analysis tools and interviews. RTPs run Lattix against each codebase and submit to RABET-V for further analysis. Interviews are conducted to confirm the existence of security services and analysis by accredited assessor organizations.

Inputs:

- Software BOM

Outputs:

- Lattix Data Model
- Software Level Scores

Build Architecture Model

Creates an architecture model containing the components, trust boundaries, and interfaces identified during the system and software architecture analysis. Security services scores are assigned at each point of use (e.g., component, trust boundary).

Inputs:

- Reliability Scores
- Security Services
- Software BOM
- Software Level Scores
- System Architecture
- System Level Scores

Outputs:

- Architecture Review Report
- Point of Use Scores

Construct architecture review workbook

Import scoring from the scoring instrument and run calculations. Thoroughly review the updated scores, looking for missing or incorrectly scored controls. Address any discrepancies by checking notes or consulting with the RTP.

Inputs:

- Depth Score
- Point of Use Score

Outputs:

- Architecture Review Workbook
- Consolidated Architecture Scores

Submit and Review Assessment

Upload all documents to the RABET-V Portal and circulate for feedback with the RABET-V Administrator and RTP.

Inputs:

- Architecture Review Workbook
- Lattix Data Model
- SARIF Report

Analyze Third-Party Component Details

The third-party component details describe the RTP's approach to managing supply chain risk. This includes whether the organization has selected third-party software components with a history of known vulnerabilities, and how the organization maintains traceability and assurance of third-party and open-source software throughout the lifetime of the software.

When considering parts of the overall solution that are not developed internally, each unique version of the following will be considered an individual component of the system:

1. Operating System
2. Framework
3. Third-party API
4. Embedded Third-party Library
5. Hosting Software/Service (e.g., IIS, Docker, Elastic Beanstalk, Azure App Service)
6. Database (stored functions and procedures will be treated as a part of the software application)
7. File Storage System/Service
8. Network Appliance (virtual or physical)
9. External Device Driver/Firmware

A replacement or major version change to one of these components will be treated as a change type subject to iteration testing per the test plan determination.

The RTP should detail initial and ongoing vetting procedures for third-party providers and components (if not covered in the process descriptions), including open-source software and libraries. Vetting should include fit for the provider as well as security and reliability. Management of third parties includes the approach to policies, service level agreements (SLAs), reputation, maintenance, and past performance of third-party software and services.

Third-party libraries will be processed through automated SBOM tools. RTPs are required to facilitate the ingestion of software libraries through designated tooling. RTPs should ensure these tools are permissible within their environments and should contact the administrator with any questions about the tools.

8.2 Architecture Maturity Rubric

The architecture assessment results in maturity scores that indicate how well the product's architecture is built to support each security service. These scores do not indicate the quality of the security services used, but how well the architecture is designed to resist attacks, protect data and functionality, and accommodate changes without impacting the security services used.

The architecture maturity rubric provides a maturity score for each of the ten security control families. The scores range from 0 to 3, where 3 is the best.

The architecture maturity rubric scores across the four measures below.

8.2.1 Reliability

The component (or the substantial logic thereof) is provided by a reputable party and actively maintained.

- 0 – Unvetted component, written in-house with minimal documentation or third-party component that is uncommon and/or not actively supported
- 1 – Vetted component used, but may not be a current version or actively supported
- 2 – Mature, vetted component used with multiple active contributors; configured by secure best practices/guidelines
- 3 – Mature, vetted component used that is actively supported or approved by a professional community/organization, and is enforced by technical or procedural controls

8.2.2 Manageability and Consistency

The component is: centrally managed by the provider, configurations are tuned with best practices, configurations are enforced, and the configuration is under full change management with attribution.

- 0 – Component does not exhibit any of the criteria
- 1 – Component exhibits one or two criteria
- 2 – Component exhibits three of the criteria
- 3 – Component exhibits all four criteria

8.2.3 Maintainability: Modularity

The component is segregated from other components at the system level and dedicated to providing its security service

- 0 – no segregation, not separated into own library
- 1 – separated into a library (inclusive of namespace segregation)
- 2 – separated process, same execution environment as a protected component
- 3 – separate unit of deployment (cloud service, or physically)

8.2.4 Maintainability: Isolation (Composite Service Only)

Access to the security service component is mediated through a central software component.

- 0 – No use of façade or proxy class
- 1 – Partial use of façade or proxy class
- 2 – Consistent use of façade or proxy class
- 3 – Invocation of security service is handled by a global handler, framework, or platform (i.e. it is written in such a way that its usage is guaranteed)

8.2.5 Depth

A component is segregated from other components and reusable inside other components. Components are complementary to provide a consistent, layered defense for the overall system. There should not be multiple versions or flavors variations of the security service component unless absolutely necessary.

- 0 – Components coverage is lacking and/or haphazardly applied
- 1 – Component coverage has gaps, is managed inconsistently, and is not segregated
- 2 – Component coverage has minimal gaps, some layering and segregation, and part of a repeatable process
- 3 – Components are intentional, built into layers, part of a repeatable/auditable process, and tested regularly

8.3 Rubric Configuration

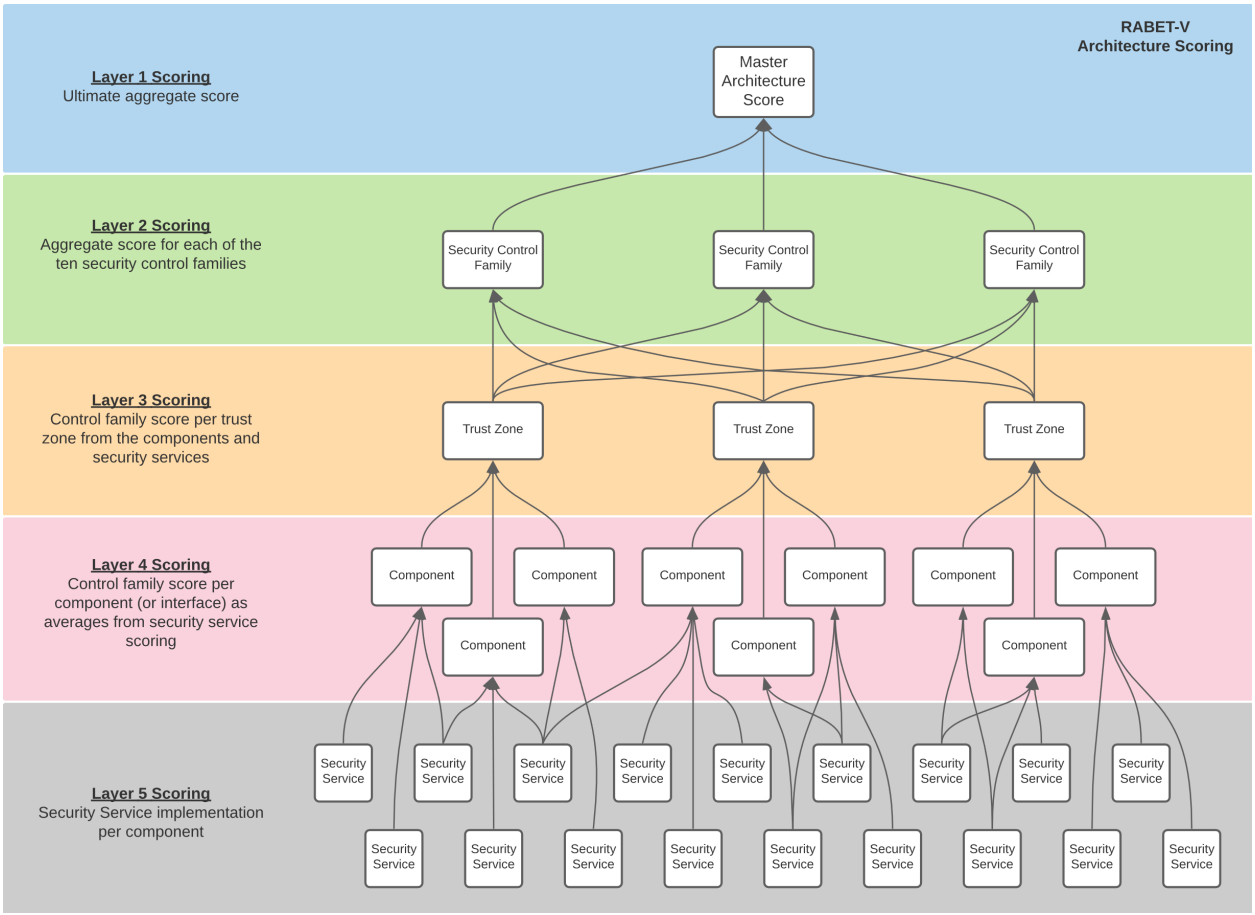
Each use of a security service is scored separately (except Depth). For example, if `Log4Net` and `EnterpriseLibrary.Logging` were used as logging and alerting services, each would be scored separately across the measures below.

Scoring is based on three measures, with maintainability broken down into modularity (for system-level services) and isolation (for software-only or composite services). Depth is scored once per security service type, at the aggregate control family level only.

Table 1: Rubric configuration per use of security service provider

Type	Reliability	Consistency	Modularity	Isolation	Example
Transparent	x	x	x		Firewall
Composite	x	x	Service Only	Software Only	Azure AD integrated with App

Rubric scoring is applied to each security service at its point of use. If the same security service is used by different components, it will receive separate scores. Scores are rolled up by trust boundary, then by security control family; finally an aggregate score is derived.



8.4 Architecture Baseline Scoring

The architecture baseline is a combination of a minimum score for each of the ten security control families along with a minimum overall baseline maturity score.

The overall baseline for the architecture maturity score is 1.50.

The table below lists the baseline scores required for each of the security control families that are measured in the architecture assessment, along with the overall score to be considered for the verified status.

Security Control Family	Baseline Score
Authentication	1.50
Authorization	1.50
Boundary Protection	2.00
Data Confidentiality and Integrity	1.50
Injection Prevention	1.25
Logging Alerting	1.50
Secret Management	1.50
System Availability	1.50
System Integrity	1.50
User Session	1.25
Overall Score	**1.50**

CHAPTER

NINE

TEST PLAN DETERMINATION

This activity takes the results from previous activities and builds a unique test plan for each product, which stays valid as long as there are no changes impacting the *organizational maturity* or *architecture maturity* scores. If there are changes to scores during the current *RABET-V iteration*, the test plan determination must be performed again.

The test plan is a crosstab decision table. Artifacts from earlier activities, such as the *submission review*, *organizational assessment*, and *architecture assessment* serve as inputs to the table. The output of the test plan determination is a set of testing rigors to be used during *product verification*. A testing rigor is determined for each *control family*.

These testing rigors are **`Full`**, **`Basic`**, and **`Streamlined`**. The names reflect the rigor that applies to confirm the effectiveness of the control family, with `Full` applying the most rigor and `Streamlined` the least.

The chosen testing rigor for a given *control family* is based on the change types identified for the product's current iteration and the organizational maturity and architecture maturity scores for the product. For instance, change types that indicate changes to security service components will require higher scores to receive `Basic` or `Streamlined` testing. Minor changes may receive less testing even with relatively lower scores.

Based on initial findings during the product verification activity, some tests may be made more rigorous than indicated in the test plan, but they cannot be made less rigorous.

The `Full` testing rigor is testing all the *security requirements* in the security control families for all the *security services*. This level of rigor is used on initial iterations, future iterations if the overall organizational and architecture maturity scores are too low to allow for `Basic` or `Streamlined` testing, or for certain change types.

The `Basic` testing rigor is used with sufficently good maturity scores from the organizational and architecture scores from the most recent assessment. This level of rigor includes the level one requirements plus the claimed requirements that represent 50% of the remaining requirements at levels two and three for each security control family that is impacted by application changes since the last iteration.

The `Streamlined` testing rigor is used with excellent maturity scores from the organizational and architecture scores from the most recent assessment. This level of rigor includes the level one requirements plus the claimed requirements that represent 20% of the remaining requirements at levels two and three for each security control family that is impacted by application changes since the last iteration.

9.1 Inputs

- Change Type
- Organizational Maturity Score
- Architecture Maturity Score

9.2 Outputs

- Product Test Plan

9.3 Workflow

9.3.1 Review assessment scores

Organizational assessment scores and architecture assessment scores serve as inputs.

The architecture maturity score for each RABET-V control family form the column headers of the table. The rows of the table list the change types. Each change type is associated with an organizational assessment score. The first change type matching any of those identified during submission review uniquely selects the applicable organizational assessment score (i.e., when more than one change type applies, the highest risk one takes precedence over the others). The organizational assessment and architecture assessment scores are then summed for each control family, resulting in scores between 0.0 and 6.0.

9.3.2 Determine testing rigors

Each numeric score is converted to a testing rigor based on a predefined set of thresholds associated with the change type. These thresholds determine how high a score must be to receive a certain level of testing. For example, a product with an *Operating system patch* change type and a combined organizational and architecture score of 2.5 or greater will receive `Streamlined` testing. However, a change of *Security patch of security service component(s)* with the same score would receive `Full` testing. The test plan matrix is given below:

	Organizational + Architecture Assessment Score									
Change Type		Organizational Assessment Score Type	> 5	5 - 4.5	4.49 - 4.0	3.99 - 3.5	3.49 - 3.0	2.99 - 2.5	2.49 - 2.0	< 2.0
1	Other major or multiple change(s) to security service component(s)	Total	Full	Full	Full	Full	Full	Full	Full	Full
2	Source code change to security service component(s)	InternalDev	Basic	Full	Full	Full	Full	Full	Full	Full
3	Major configuration change to security service component(s)	EnvMgmt	Basic	Basic	Basic	Full	Full	Full	Full	Full
4	Security patch of security service component(s)	SupplyChain	Basic	Basic	Basic	Basic	Full	Full	Full	Full
5	Dependency updates for security service component(s)	SupplyChain	Basic	Basic	Basic	Basic	Basic	Full	Full	Full
6	Minor configuration change to security service component(s)	EnvMgmt	Basic	Basic	Basic	Basic	Basic	Basic	Basic	Full
7	Source code change interfacing with security service component(s)	InternalDev	Streamlined	Basic	Basic	Basic	Basic	Basic	Basic	Full
8	Source code change unrelated to security service component(s)	InternalDev	Streamlined	Streamlined	Streamlined	Basic	Basic	Basic	Basic	Full
9	3rd party software patch to a non-security sevice component(s)	SupplyChain	Streamlined	Streamlined	Streamlined	Streamlined	Streamlined	Basic	Basic	Full
10	Operating system patch	EnvMgmt	Streamlined	Streamlined	Streamlined	Streamlined	Streamlined	Streamlined	Basic	Full
11	Other software or configuration change	Total	Streamlined	Streamlined	Streamlined	Streamlined	Streamlined	Streamlined	Basic	Full

CHAPTER

TEN

PRODUCT VERIFICATION

The product verification activity is conducted by an *accredited assessor organization* and establishes the *product implementation score*. The goal is to establish that a product meets the claims the *RTP* made about it, that is: "does the product prevent unintended outcomes?"

For *initial product submissions* and extensive changes in a *product revision submission*, the full product verification process will be used to determine, or redetermine, the proper scores. For other, smaller product revisions this activity will be streamlined because the changes were determined to pose a lower risk to the system.

10.1 Methodology

For more information about what is expected for the product verification activity, see the *provider submission* activity and the *RABET-V security requirements*.

For initial product submissions, a full system test is performed. A full system test will review automated test results and perform a systemwide functional test and penetration test.

For product revision submissions, the *test plan determination activity* outlines required tests.

10.1.1 Inputs

- *Test plan*
- Component definitions from *architecture assessment*
- System-level architecture diagram
- System details from *organizational assessment*
- Product revision submission materials, if applicable

10.1.2 Outputs

- Results of verification test methods
- Product implementation score based on the product implementation rubric

10.2 Verification Methods

An accredited assessor organization will use one or more of the following techniques, as indicated in the test plan. The scope of the testing (i.e., which components to test) will also be indicated by the test plan.

10.2.1 Artifact Review

This method will review an artifact provided by the RTP. The review will look for gaps or concerns in relevant controls based on the information provided. Each type of artifact will have various indicators of acceptability. Types of RTP artifacts include:

- Automated source code unit test results
- Automated vulnerability test results
- Automated configuration verification results
- Security event audit logs
- Third-party security analysis results (automated or manual)

The artifacts must be evaluated as "reliable" during the organizational assessment activity in order to be used for product verification.

10.2.2 Automated Testing

Automated testing is a broad type of testing that relies on software to perform test routines against the product or product component. Automated testing will execute the testing software against its target and produce results which will be evaluated by the accredited assessor organization. The type of automated test will depend on the target. Types of automated testing may include:

- Configuration testing
- Vulnerability analysis
- Source code analysis
- Accessibility testing
- Browser compatibility testing

10.2.3 Penetration Testing

Penetration tests evaluate the product to find security vulnerabilities that an attacker could exploit. The scope of a penetration test may be the product's network, computer systems, hardware components, or software application(s). Penetration testing is typically a combination of manual and automated testing. Automated tools help with web application pen tests but must be used by skilled and experienced testers.

RABET-V relies on OWASP's Web Application Security Testing Guide for web application and web service penetration testing options.

In addition to a full penetration testing option, the following web application penetration testing subtypes are supported:

- Configuration and deployment
- Identity management
- Authentication
- Authorization
- Session management
- Input validation
- Error handling
- Cryptography

Limited penetration testing may be used if the changes do not warrant full penetration testing.

10.3 Product Implementation Rubric

The product implementation rubric provides a maturity score for each of the *control families* based on how well the product meets the requirements within those families. The scores range from zero to three, where three is the best.

The requirements are a binary pass or fail. Any assumptions made about the configuration or setup of the product must be documented with the result.

The scores are calculated by summing the percentage of applicable requirements that pass at each maturity level. For instance, meeting 100% of requirements at maturity level one, 25% at maturity level two, and 0% at maturity level three would result a score of 1.25.

10.3.1 Security Test Method Descriptions

- Fuzzing - Test of the application's ability to accept a wide variety of inputs without causing it to enter an unexpected or undefined state
- Penetration Testing - Testing that verifies the extent to which a system, device or process resists active attempts to compromise its security [NIST SP 800-152]
- Functional - Test that evaluates the functionality of a component against a design specification. Can be automated, but because the function will be implemented differently by each product, a custom test script may be required for each
- Web Testing - A functional test that exercises one or more parts of the web stack and verifies the expected output
- Failover and Restore Testing - Test that evaluates the resiliency of a system by making components of the system inoperable and evaluating the result
- Code Analysis - A white box test involving the use of code artifacts, such as source code or unobfuscated binaries in order to verify certain properties

- Bill of Materials (BOM) Analysis - Analysis of the bill of materials, such as software and their versions
- Configuration Audit - Test to verify that the configuration of a component is configured as required
- Data Audit - Test to verify the presence or absence of certain records, such as the inappropriate collecting of PII or the lack of authentication logs, can be combined with functional testing to provide a higher level of confidence
- Artifact Review - Review of RTP-supplied artifacts from their development, testing, integration, and deployment process or artifacts provided by the RTP'S hosting environment
- Documentation Audit - Review of the RTP-supplied documentation for presence of required content or presence of poor guidance (i.e. direction to use insecure password)
- Vendor Attestation - A statement made by the vendor indicating the existence of one or more security controls

10.3.2 Accessibility Test Method Descriptions

- Conformance - Test that validates the conformance of a component, page, or application to a specific accessibility standard. Conformance testing can be automated during development to test components and after development to test full applications. For example, tools like Accessibility Insights can check Android, web, and Windows applications, eslint-plugin-jsx-a11y can perform static analysis on React applications, axe DevTools can be used to test web applications, and SiteImprove is a paid-service that can automate accessibility, spell-checking, and readability checks on web applications
- Functional - Test that evaluates the functionality of a component against a set of accessibility expectations. This must include the ability to interact with only keyboard navigation and should include testing with assistive technology (e.g., screen reader, braille display) and plain-language analysis (e.g., ideal Flesch-Kincaid score)
- Artifact Review - Review of RTP-supplied artifacts from their automated, functional, or third-party testing
- Vendor Attestation - A statement made by the vendor indicating the adherence to one or more accessibility controls

10.3.3 Usability Test Method Descriptions

- Artifact Review - Review of RTP-supplied artifacts from their functional or third-party testing
- Vendor Attestation - A statement made by the vendor indicating the adherence to one or more usability controls

10.4 Product Verification Baseline

The product verification baseline contains all the security requirements at level one and 50% of the requirements from levels two and three combined. When the RTP completes the product claims workbook, they will identify at least 50% of the Level two and Level three requirements

from each of the control families. These claimed requirements will be part of the testing in the basic and streamlined testing scenarios.

The overall minimum baseline for verification is 106 of 153 requirements, combining all of Level one and 50% of the combined Level two and three requirements in each of the security control families.

The authentication baseline is passing all level one requirements (below) and 6 of 12 level two and three requirements.

Security Control Family	Requirement
Authentication	1.1.1 Default passwords are not used or are automatically changed as part of set up
Authentication	1.1.2 Authentication is applied consistently through the application
Authentication	1.1.3 Encrypt or hash all authentication credentials
Authentication	1.1.4 Customer admins have access to an inventory of their user accounts
Authentication	1.1.5 Implement protections against brute force attacks
Authentication	1.1.6 Require multi-factor authentication for all administrative access

The authorization baseline is passing all level one requirements (below) and 4 of 8 level two and three requirements.

Security Control Family	Requirement
Authorization	2.1.1 Platform provides an authorization system
Authorization	2.1.2 Applications and middleware should run With minimal privileges
Authorization	2.1.3 Apply the principle of least privilege
Authorization	2.1.4 Use tokens to prevent forged requests

The boundary protection baseline is passing all level one requirements (below) and 6 of 12 level two and three requirements.

Security Control Family	Requirement
Boundary Protection	3.1.1 Deny communications with known malicious IP addresses
Boundary Protection	3.1.2 Deny communication over unauthorized ports
Boundary Protection	3.1.3 Deploy network-based IDS sensors
Boundary Protection	3.1.4 Document traffic configuration rules
Boundary Protection	3.1.5 Use MFA for managing network infrastructure
Boundary Protection	3.1.6 Configure perimeter devices to prevent common types of attacks
Boundary Protection	3.1.7 Disable wireless access on devices if it is not required
Boundary Protection	3.1.8 Documentation clearly identifies wireless capabilities
Boundary Protection	3.1.9 Provide dedicated wireless networks
Boundary Protection	3.1.10 Disable wireless peripheral access to devices

The data confidentiality and integrity baseline is passing all level one requirements (below) and 8 of 15 level two and three requirements.

Security Control Family	Requirement
Data Confidentiality	4.1.1 Use valid HTTPS certificates from a reputable certificate authority
Data Confidentiality	4.1.2 Encrypt transmittal of username and authentication credentials
Data Confidentiality	4.1.3 Use the strict-transport-security header
Data Confidentiality	4.1.4 Disable data caching using cache control headers and autocomplete
Data Confidentiality	4.1.5 Updated TLS configuration on servers
Data Confidentiality	4.1.6 Use TLS everywhere
Data Confidentiality	4.1.7 Disable HTTP access for all TLS enabled resources
Data Confidentiality	4.1.8 Do not disclose too much information in error messages
Data Confidentiality	4.1.9 Display generic error messages
Data Confidentiality	4.1.10 Store user passwords using a atrong, iterative, salted hash

The system availability baseline is passing all level one requirements (below) and 3 of 6 level two and three requirements.

Security Control Family	Requirement
System Availability	5.1.1 Ensure regular automated backups
System Availability	5.1.2 Backup data should be restorable
System Availability	5.1.3 Local distributed storage capability
System Availability	5.1.4 Local distributed processing capability

The injection prevention baseline is passing all level one requirements (below) and 4 of 7 level two and three requirements.

Security Control Family	Requirement
Injection Prevention	6.1.1 Use secure HTTP response headers
Injection Prevention	6.1.2 Validate uploaded files
Injection Prevention	6.1.3 Set the encoding for your application
Injection Prevention	6.1.4 Validate all input

The logging and alerting baseline is passing all level one requirements (below) and 7 of 14 level two and three requirements.

Security Control Family	Requirement
Logging and Alerting	7.1.1 Activate audit logging
Logging and Alerting	7.1.2 Ensure adequate storage for logs
Logging and Alerting	7.1.3 Log all authentication activities
Logging and Alerting	7.1.4 Log all privilege changes
Logging and Alerting	7.1.5 Do not log inappropriate data
Logging and Alerting	7.1.6 Store logs securely
Logging and Alerting	7.1.7 Log and alert on changes to administrative group membership

The secret management baseline is passing all level one requirements (below) and 3 of 5 level two and three requirements.

Security Control Family	Requirement
Secret Management	8.1.1 Don't hardcode credentials
Secret Management	8.1.2 Store credentials securely
Secret Management	8.1.3 Credentials for non-production and production environments are different

The system integrity baseline is passing all level one requirements (below) and 6 of 12 level two and three requirements.

Security Control Family	Requirement
System Integrity	9.1.1 Install the latest stable version of any security-related updates on all network devices
System Integrity	9.1.2 Ensure anti-malware software and signatures are updated
System Integrity	9.1.3 Configure devices to not auto-run content
System Integrity	9.1.4 Use port protectors on unused ports
System Integrity	9.1.5 Configure anti-malware scanning of removable devices

The user session baseline is passing all level one requirements and 3 of 6 level two and three requirements.

CHAPTER

ELEVEN

REPORTING PROCESS

The *RABET-V administrator* creates a report for the *RTP* containing scores from the *architecture assessment*, *organizational assessment*, and *product verification*, a verification status, and recommendations for improvement. The administrator will send the RTP two versions of this report: a full report with detailed appendices and a roadmap for ways to improve and a short report verifying that the baseline requirements were met. Agencies can request the short report during procurement processes, as part of contract management, or during annual security reviews.

The *RABET-V public listing site* contains a list of verified products containing the tech provider name, the product version, some configuration details, and verified status. RTPs will have the option to opt out of publicly listing their product if they choose.

11.1 Inputs

- Results from all relevant activities

11.2 Outputs

- RABET-V product report and appendices
- Status of verified or not verified

11.3 Workflow

Since each RABET-V activity generates artifacts with product or organization recommendations and scores, the RABET-V administrator create a summary report of all the findings and assign the product a **Verified** or **Not Verified** status. The report can also be in one of three states: **Draft**, **Conditional**, and **Final**. The combination of the product status and the state of the report determines the overall RABET-V assessment status.

After the RABET-V administrator finish a report, its status is *Draft*. The report is then shared with the *RTP* to allow the RTP to raise potential content disagreements. The RTP has ten days to raise any issues with the report. If the RTP disputes any findings or communicates that it plans to resubmit the product for testing in the current iteration, its status changes to *Conditional*. The RTP then has 30 days to resubmit the product. If an RTP submits a product for retesting in the current iteration—and the RABET-V administrator accepts it as a part of the current

iteration—then the report generated from the newly tested product changes back to *Draft*, and the RABET-V cycle starts one additional time. If an RTP accepts the report as-is or the acceptance or resubmission period lapses, the report's status changes to *Final*. When the report enters this stage, the report is signed by the RABET-V administrator and sent to the RTP.

If the product itself is given a *Not Verified* status, the RTP can assess the changes required to remediate the deviations. If they re-submit within the allowed time, they may be able to incorporate it into the same submission. This is at the RABET-V administrator's discretion. A cursory architecture analysis can evaluate the submission delta and consider whether it is scoped only to address the deviations. If it is appropriately scoped, it may fall under this provision. Otherwise, it must be regarded as a separate iteration.

Once the remediation submission is evaluated and through product verification, the verification outputs will be assessed to determine if the deviations have been resolved. If so, the product may move to *Verified*. Otherwise, the product is *Not Verified*, and the iteration is ended.

11.4 Report Statuses

Draft
: After the RABET-V administrator finish an assessment report, its status is **Draft**. The report is then shared with the RTP to discuss potential content issues. The RTP has 10 days to communicate any disagreement with the findings or indicate that they will submit a product for the current iteration. At that point, the Draft status changes to *Conditional*. If the RTP signals that they accept the report or the 10-day period lapses with no communication from the RTP, the report status changes to *Final*, and the assessment is complete.

Conditional
: If the RTP disputes any findings or communicates that it plans to resubmit the product for testing in the current iteration, its status changes to **Conditional**. The RTP must suggest changes or resubmit the product within 30 days. If the RTP provides changes to the report, the RABET-V administrator adjudicate the changes within 10 days, and the report will be changed to *Final*. If the RTP submits a product for testing within the current iteration, the reassessment results are folded into the report, and its status is reverted to *Draft* one final time. If the 30-day period lapses without the RTP resubmitting the product or the RTP indicates that they accept the report in its current form, the report status changes to *Final*, and the assessment is complete.

Final
: If an RTP accepts the report or the acceptance or resubmission period lapses, its status changes to **Final**.

11.5 RABET-V Product Statuses

Not Verified
: **Not Verified** means:

  - While the product is likely to perform as described, the RABET-V process identified at least one significant deficiency.
  - The RTP is expected to remediate the deficiency(s) and re-submit within 30 days.

- Suppose no other changes are made to the product. In that case, the re-submission is considered part of the same submission and, upon review, can change the RABET-V product status to *Verified*. Resubmission may still undergo an expedited RABET-V process. For example, if organizational processes meet or exceed the baseline and remain the same, no organizational assessment needs to be performed. Additionally, depending on the change, the product may be able to undergo an expedited architectural assessment and product verification.

Verified

A **Verified** status means the product will likely perform as described in the expected usage operating environment. To achieve a verified status, the organizational assessment, architecture assessment, and product verification results must meet or exceed the baseline in each area.

11.5.1 Product Report Generation

Report Template

The RABET-V results summary provides scores for organizational maturity, architecture maturity, and product implementation. For revision submissions, it will include any change from the previous submission.

Organizational maturity: quality of the RTP's product development practices. The organizational assessment maturity result reflects the extent to which this is achieved for each of these areas:

- Governance
- Design
- Implementation
- Verification
- Operations
- Human factors

Architecture maturity: the reliability of the product's such that changes to one product feature or service will not have unintended implications for other aspects of the product. The architecture assessment maturity result reflects the extent to which this is achieved for each of the control families.

Product implementation maturity: the quality of the product's capabilities to meet the claims the RTP made about it. The product verification result reflects the extent to which this is achieved for each of the control families.

Product (Revision) Summary: details about the product that were submitted including its description, expected usage (i.e., use cases), version number(s), etc. This includes the change list for *product revision submissions*.

Verification Methods: a description of how the system was tested to include verification methods used in the testing.

Maturity Trends: a description of what caused a change for any product or process maturity level that changed.

Appendices: as needed.

CHAPTER

TWELVE

ASSESSOR ACCREDITATION

Purpose: This document provides the process and requirements for attaining and maintaining status as an *accredited assessor organization* under the RABET-V program.

CHAPTER

THIRTEEN

ELIGIBILITY

Organizations that may apply to become accredited assessor organizations under the RABET-V program include but are not limited to: private companies and corporations, non- and not-for-profit organizations, universities and other academic institutions, and government entities. For the purposes of this section, all such entities will be referred to as an organization and must meet the requirements described in this document.

13.1 Basic Eligibility

Basic eligibility requirements include:

1. Declaration of any ownerships or parent companies from outside of the United States. Eligibility based on any such ownership will be made on a case-by-case basis at the sole discretion of the *RABET-V administrator*
2. The organization is based in the United States and has operations on United States soil
3. All individuals performing work under the assessments are U.S. citizens unless specifically agreed to in writing by the RABET-V administrator
4. All work under the assessments is performed on U.S. soil, including virtual and cloud resources, unless explicitly approved by the RABET-V program
5. The organization and its employees having satisfactorily passed a background check within the previous year and having no known impediments that would prevent successfully completing a background check
6. The organization carries insurance as specified in the assessor agreement
7. There is no financial interest in any RABET-V *registered technology provider*
8. The organization is not actively developing technology for commericial use that may be considered as part of the RABET-V program, including designing, writing documentation, or building, coding, or implementing such a technology
9. The organization is not an EAC registered manufacturer

13.2 Requirements for Maintaining Eligibility

Once accredited, organizations **MUST** report any change in the following to RABET-V as soon as practicable and within 30 days:

1. Any change in ownership or parent companies that include entities either from outside of the United States, greater than 10% of total ownership, or both, or otherwise violates the eligibility requirements
2. Any significant changes relevant to its accreditation, in any aspect of its status or operation relating to:
    - legal, commercial, organizational, or ownership status
    - organization, top management, or key personnel, including authorized pepresentative, approved signatories, and any individuals with software licenses related to the RABET-V program
    - resources and location, including equipment, facilities, and working environment, where significant
    - scope of accreditation, or other matters that may affect the assessor's ability to comply with RABET-V requirements

13.3 Preventing Conflicts of Interest and Impropriety

The organization **MUST**:

1. Prohibit and prevent conflicts of interest or the appearance of conflicts of interest for the organization and all of its employees
2. Refrain from soliciting or receiving gifts from any producer of technology in conformance with federal employee rules for gifts from outside sources, set forth at 5 CFR 2635 sections 201-205 and 301-304
3. Abide by the policies and procedures set forth within this Program Manual

13.4 Tailored Use Eligibility

At times, some states or localities may request that additional requirements be applied only to those technology providers seeking to operate in their respective jurisdiction(s). One potential example of this is a university that conducts assessments for its home state.

In those cases, an agency may request a tailored use phase of the RABET-V assessment, which will be managed on a case-by-case basis. Organizations that are not accredited through the RABET-V accreditation program may be specified for assessments under such a tailored use policy, but their activities will be limited to those defined under that specific tailored Use policy. Organizations specified to conducted assessments under a tailored use policy that are accredited through RABET-V have no such restrictions and are treated like any other accredited assessor.

The RABET-V administrator discourages tailored use as they can slow reviews and add additional cost, but supports them when needed, particularly early in transitions to relying on the RABET-V program while we work to incorporate state and locality needs into RABET-V.

13.5 Curing of Lapses in Eligibility

An accredited organization that is found to no longer meet the requirements in this document will generally have 30 days to cure any issues. More time may be granted in the event of demonstrated progress.

At its discretion, the RABET-V administrator may limit the organization's assessments while in the cure process, to include pausing or canceling current assessments and not assigning new assessments. If an assessment is paused or canceled due to eligibility issues, the assessor may be liable for any costs incurred to retest and/or complete assessments.

CHAPTER

FOURTEEN

ORGANIZATIONAL COMPETENCY

To achieve and maintain accreditation, the relevant organizational unit conducting assessments must meet organizational competency requirements as described in this section. These include demonstrating competency through a minimum information security posture, technical capabilities for resources employed in assessments, and specific capabilities related to RABET-V assessments.

Organizations **MUST** maintain a modern cybersecurity posture throughout their enterprise. This includes all enterprise assets, networks, and personnel. To provide evidence of their organizational competence and cybersecurity posture, assessors must provide the RABET-V administrator documentation confirming that at least one of the following has been met:

1. Leveraging the CIS Controls Self Assessment Tool (CIS CSAT). This tool helps enterprises assess, track, and prioritize their implementation of CIS Controls v7.1 and v8. Assessors must obtain a minimum of Implementation Group 1 and provide evidence via a CIS CSAT report.
2. Obtaining an external, third-party assessment of organizatonal cybersecurity controls in accordance with at least one of the major following security frameworks:
    - CIS Controls. Conformance will be determined by the RABET-V administrator based on a minimum of achieving implementation group one
    - ISO/IEC 27001. Enterprises must achieve the certification. There are a family of standards surrounding ISO 27001. Achieving certification with any of the recognized national variants of ISO/IEC 27001 is equivalent for certification to ISO/IEC 27001
    - Control Objectives for Information Technology (COBIT)
    - Payment Card Industry (PCI) Data Security Standard
3. Obtaining compliance or accreditation to any of the following. Achieving this will require submission to the RABET-V program of associated policies against which the organization was assessed to ensure appropriate information security measures have been implemented
    - National Voluntary Laboratory Accreditation Program (NVLAP) Voting System Testing accreditation (NVLAP 150-22). NVLAP accreditation signifies that a laboratory has demonstrated that it operates in accordance with NVLAP management and technical requirements pertaining to quality systems; personnel; accommodation and environment; test and calibration methods; equipment; measurement tractability; sampling; handling of test and calibration items; and test and calibration reports

- ISO 9001 compliance. Compliance with this standard ensures that an enterprise is leveraging a set of policies, procedures, and processes that guide an organization's activities and operations to meet the needs and expectations of its customers and stakeholders
- Conformance with another, related framework or control set as determined at the discretion of the RABET-V administrator. If an assessor requests and is granted acceptance via a framework that is not listed here, that framework will be added to the next version of this manual. This promotes flexibility as new frameworks emerge

14.1 Technical Capabilities

All organizations **MUST** demonstrate that they can provide a team composed of employees or contractors with the following:

1. Skills commensurate with the scope of work, such as a technical degree (e.g., a degree in computer science, computer engineering, electrical engineering, human factors, software engineering, etc.), similar technical discipline, or equivalent experience (e.g., professional certification, etc.)
2. Knowledge of test methods applicable to the RABET-V program
3. Knowledge of relevant standards affecting their area of expertise

In addition to the organizational requirements listed above:

14.1.1 Organizational Assessors Require One (or more) of the Following:

1. Designation as a SAMM practitioner
2. Expertise in organizational maturity models such as Software Assurance Maturity Model (SAMM) or Building Security in Maturity Model (BSIMM) or ISO 27001
3. Experience assessing or building and managing software application security or secure development

14.1.2 Architecture Assessors Require:

1. Knowledge of and experience developing in two or more popular languages used by technology vendors (e.g. .NET/C#, Java, Python, Objective-C/Swift) including popular third party security service libraries and mitigation approaches
2. Knowledge of common web application security vulnerabilities (OWASP Top 10, SANS 25, etc.)
3. Ability to identify and confirm the proper use of design patterns, including object-oriented and gang of four (GOF) (e.g. Façade, Proxy, IoC, etc.)
4. Experience with secure coding practices, such as input validation, error handling, and encryption
5. Experience with static and dynamic code analysis and related tooling

6. Experience working with vulnerability management, software composition analysis (SCA) and software bill of materials (SBOM) analysis tooling
7. Experience with conducting system architecture reviews of traditional monolith and modern cloud-based architecture
8. Experience with conducting threat modeling and diagraming of different types of architecture patterns

14.1.3 Product Verification Assessors Require:

1. A minimum of 3 years of experience in penetration testing or a related cybersecurity role, with specific experience in critical infrastructure security preferred
2. Experience with various types of product testing, including hardware, software, web applications, and embedded systems
3. Knowledge of cloud infrastructure and testing
4. The ability to write test cases based on the documented requirements and the system to be tested, and complete the test cases
5. Familiarity with various programming languages (e.g., Python, Ruby, Java, C/C++, and JavaScript) and operating systems (e.g., Windows, Linux, macOS)
6. Proficiency in using popular penetration testing tools and frameworks, such as Metasploit, Burp Suite, Nmap, and Wireshark
7. Knowledge of secure coding practices, common vulnerabilities, and industry standards, such as the OWASP top ten
8. Relevant certifications, such as Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH), or Global Information Assurance Certification (GIAC), are encouraged
9. Excellent analytical, problem-solving, and communication skills, with the ability to clearly articulate complex security issues to both technical and non-technical audiences

CHAPTER

FIFTEEN

CONFIDENTIALITY AND WORK PRODUCTS

All organizations must exhibit proper management of the sensitive data that is part of the RABET-V program. Further details will be provided in the accreditation and assessment agreements but, in general, organizations **MUST**:

1. Maintain strict data separation and confidentiality regarding information from different assessments
2. Adhere to any non-disclosure agreements that may be part of the accreditation program and each assessment
3. Adhere strictly to terms regarding data retention, protection, destruction, and sharing
4. Acknowledge that organizations conducting assessments will be operating under the direction of the RABET-V administrator creating works for hire and assignment
    - As such, organizations are expected to produce high level test plans that will be the property of The Turnout. These plans include: description of system; analysis of which requirements applied; description of tests run to fulfill requirements
    - Organizations are expected to produce assessment reports that meet the requirements of the RABET-V administrator that will be the property of The Turnout
5. Organizations are not prohibited from performing technology testing outside of the RABET-V program so long as such activities do not conflict or appear to conflict with RABET-V assessments

CHAPTER

SIXTEEN

APPLICATION PROCESS

Accreditation is a two-step process. To appy for accreditation an organization **MUST**:

1. Meet all the eligibility and organizational competency requirements and have staff or contractors on the team who meet the technical requirements listed above
2. Maintain key personnel that meet the requirements for one or more of the following: organizational assessments, architecture assessments, or product verifications

An accredited organization may choose to accredit assessors and conduct just one of the RABET-V assessments, or several.

As part of the accreditation application, assessing organizations **MUST** agree to:

1. Participate in an initial review that ensures the organization and individual assessors meet the requirements outlined above, which may include documentation review, interviews with relevant staff and contractors, and assessments of individual assessor competencies
2. Participate in a training program crafted for the assessments the organization would like to conduct
3. Participate in proficiency testing as required
    - During an initial probationary period of three RABET-V engagements, the Administrator will continually review work product to it meets expectations, and that training was adequate
    - Accredited assessors are required to complete an annual attestation that the information contained in the original application is still valid
    - In addition, every two years the RABET-V program will conduct an audit that includes a verification of work product and individuals that contributed to any reports or assessments on behalf of the accredited assessor

Approval for accredited organizations and assessors is at the discretion of the RABET-V administrator.

CHAPTER

SEVENTEEN

QUALITY MONITORING

The RABET-V adminstrator will perform regular monitoring of assessor's output. This may include on-site visits, reviews of test methods, test protocols, interview questions, and documentation. In order to support this, The RABET-V administrator will randomly review assessment outputs from assessors for quality, efficiency, and sufficiency using a variety of methods to include manual inspection and statistical review. The goal of this monitoring is to:

1. Maintain a high level of quality throughout the program
2. Ensure that that the procedures of this manual are followed
3. Maintain a reasonable level of consistency of testing between assessors

CHAPTER

EIGHTEEN

RABET-V GLOSSARY

Accredited Assessor Organization
: A business entity who has gone through the accessor accreditation process and guides the assessment of a product to generate maturity scores for the RTP.

Activity
: A self-contained aspect of the RABET-V program. Each activity has a process with inputs, outputs, and a workflow.

Architecture Assessment
: An evaluation of a *product's* architectural support for the RABET-V security control families by an accredited assessor organization to determine how mature the architecture is that supports each *security service*.

Architecture Maturity Score
: A numerical value assigned by an accredited accessor organization that examines the product's components at both the system and software levels to develop a picture of risk and risk mitigation to answer the questions "how well-designed is the architecture underlying the product?".

BPMN
Business Process Model and Notation
: A "graphical notation that depicts the steps in a business process. BPMN depicts the end to end flow of a business process. The notation has been specifically designed to coordinate the sequence of processes and the messages that flow between different process participants in a related set of activities." See the BPMN website.

Component
: (RABET-V Component Diagrams) A modular unit included in one or more products' that interacts with its environment using well-defined interfaces.

Composite Service
: A security service component that is composed of two or more coupled security service components in order to provide functionality. Most composites will consist of a security service that surfaces at the system level (core service), and an adaptor that uses or implements that service (dependent service).

Function
: A discrete piece of functionality provided by the *product*. Represented as a "*port*" in the UML Component diagram.

In-scope Services
A service component of the product that executes any of the control family functions.

Initial Product Submission
A first-time submission for a *product* to the RABET-V process that includes statements about the product and the RTP that will be used throughout each RABET-V activity.

Isolation
The "degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified" (ISO 25010:2011).

Modularity
The "degree to which a system or computer program is composed of discrete components such that a change to one component has minimal impact on other components" (ISO 24765).

Organizational Assessment
An evaluation of the quality of a *registered technology provider's* product development practices by an *accredited assessor organization* to determine how mature a product's software assurance is including usability and accessibility.

Organizational Maturity Score
A numerical value assigned by an accredited accessor that measures the quality of a technology provider's product development practices to answer the question "how good is the organization at developing technology products?".

Port
A bundle of interfaces that provides system functionality.

Product
A technology submitted to RABET-V for verification.

Product Implementation Score
A numerical value assigned by an accredited accessor that determines the ability for the system to prevent unintended actions or output to answer the question "does the product prevent unintended outcomes?"

Product Revision
A specific version of the *product* submitted to RABET-V.

Product Revision Submission
A submission by the Registered Technology Provider that includes all changes being made to a product that has already been through the RABET-V process.

Product Submission
The set of information and artifacts provided by the Registered Technology Provider necessary to initiate or revise the RABET-V process.

Product Verification
An attestation of whether a product prevents unintended outcomes outlined in claims made by the *registered technology provider's*.

RABET-V Administrator
: The organization responsible for overseeing and executing the RABET-V Program. The Turnout is the administrator for the program.

RABET-V Iteration
: A complete cycle through the RABET-V activities with a unique *product revision*. The first iteration is called the Initial Iteration.

RABET-V Portal
: A platform for accredited assessors, RTPs, and state/local jurisdictions to register for the RABET-V program and communicate about RABET-V activities. Contact the *RABET-V Administrator* to register or log-in to the Portal.

RABET-V Public Listing Site
: A website maintained by the *RABET-V Administrator* that identifies current RABET-V Listed Products.

RABET-V Strategic Advisory Committee
: A group composed of representatives from national associations, the sector coordinating committee, subject matter experts, and members of the accessibility and disability communities who provide feedback on the strategic direction of RABET-V.

Reliability
: The "degree to which a system, product or component performs specified functions under specified conditions for a specified period of time" (ISO 25010:2011).

Required Security Services
: Mechanisms used to provide confidentiality, integrity authentication, source authentication and/or support non-repudiation of information.

RTP
Registered Technology Provider
: An organization that develops technology and has registered for the RABET-V program.

Security Control Family
: A group of security services that supports the security goals. See *RABET-V control families*.

Security Enclave
: Collection of components connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location, according to the UAF.

Security Service
: A capability that supports one, or many, of the security goals (NIST definition). Multiple security services (or controls) are collected in a *security control family*.

Security Services Architecture
: An architectural view created in the architecture assessment which identifies components and maps them to the 10 *security control families*.

Services
: A system level component that provides data processing capabilities.

Test Plan
: A unique assessment scheme for each product built from the results of the organizational and architecture maturity scores, which stays valid as long as there are no changes impacting the organizational and architecture maturity scores during the current RABET-V iteration.

Transparent Service
: A security service that is not directly or indirectly invoked by the system.

CHAPTER

NINETEEN

RABET-V CONTROL FAMILIES

RABET-V defines control families that are used throughout the RABET-V process to help evaluate products. The security control families enumerated below are currently used throughout the RABET-V program, and usability and accessibility control families are currently under development. RABET-V is designed to extend to other areas as needed and may include additional control families in the future.

19.1 Security Control Families

1. **Authentication:** Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system (NIST FIPS 200)
2. **Authorization:** The right or a permission that is granted to a system entity to access a system resource (NIST SP 800-82 Rev. 3)
3. **Injection Prevention:** The sanitization of data input and output (possibly by rejecting unacceptable inputs or outputs) to ensure malicious executable code is not executed
4. **Key/Secret/Credentials Management:** The activities involving the handling of cryptographic keys and other related security parameters (e.g. passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction (NIST CNSSI 4009-2015)
5. **User Session Management:** The act of establishing, protecting, and, when necessary, demolishing the persistent interaction between a subscriber and an end point (adapted from NIST SP 1800-17b)
6. **Logging/Alerting:** The systemic management and monitoring of the events—the discrete interactions that happen within and between systems, applications, and users—occurring within an organization's systems and networks (adapted from NIST SP 800-92)
7. **Data confidentiality and integrity protection:** Assurance that the data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. Adapted from NIST SP 800-33, data confidentiality deals with protecting against the disclosure of information by ensuring that the data is limited to those authorized or by representing the data in such a way that its semantics remain accessible only to those who possess some critical information (e.g., a key for decrypting the enciphered data) (NIST SP 800-13)

8. **Boundary protection:** Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g. gateways, routers, firewalls, guards, encrypted tunnels) (NIST SP 800-53 Rev. 5)
9. **System availability protection**: The property that data or information is accessible and usable upon demand by an authorized person (NIST SP 800-66 Rev. 1)
10. **System integrity protection:** The activities based around protecting the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental (NIST SP 800-27 Rev. A)

19.2 Accessibility Control Families.

Accessibility requirements are grouped into control families based on the Web Content Accessibility Guidlines (WCAG) principles that provide the foundation for Web accessibility. RABET-V adopts the four principles of WCAG, perceivable, operable, understandable, and robust, as control families for accessibility.

There are three levels of WCAG 2.1 conformance: A (lowest), AA, and AAA (highest). RABET-V identifies conformance with each Level in its reports. For instance, if the product meets Level AA, this will be indicated in the product's final report.

1. **Perceivable:** Information and user interface components must be presentable to users in ways they can perceive
2. **Operable:** User interface components and navigation must be operable
3. **Understandable:** Information and the operation of user interface must be understandable
4. **Robust:** Content must be robust enough that it can be interpreted by a wide variety of user agents, including assistive technologies

19.3 Usability Control Families

Guiding controls for usability are based on ISO 9241-210.

1. **Understandable:** The design is based upon an explicit understanding of users, tasks, and environments
2. **User Integrated:** Users are involved throughout design and development
3. **Evaluative:** The design is driven and refined by user-centered evaluation
4. **Holistic:** The design addresses the whole user experience

CHAPTER

TWENTY

SECURITY REQUIREMENTS

The RABET-V security requirements form the backbone of the RABET-V program. Pulled from several national security standards for non-voting equipment, these 153 discrete security requirements are tailored to the product throughout the RABET-V assessments. Some security requirements apply to all components and product types, and others apply to only some components or product types, such as web components, hosted components, or on-premises components. All products must meet certain baseline security requirement standards to achieve verified status. Each of the ten overarching requirements are stratified into three maturity levels to ensure a focus on growth throughout the RABET-V process. *Accredited assessor organizations* use security requirements directly or indirectly in each of the three main RABET-V *activities*: the *architecture assessment*, the *organizational assessment*, and the *product verification*.

The following security requirements reference three national security standards for non-voting equipment: CIS Security Best Practices for Non-Voting Election Technology, CIS Controls, and NIST 800-53r5.

20.1 1. Authentication Requirements

20.1.1 1.1 Maturity Level 1

1.1.1 Requirement: Default passwords are not used or are automatically changed as part of set up

Details: Before deploying any new asset or instances, change all default passwords to have strong values consistent with policy.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.4.2
- CIS Controls v8 5.1
- NIST 800-53r5 AC-2

1.1.2 Requirement: Authentication is applied consistently through the application

Details: Users are authenticated consistently through the application using an authentication service, with variations for different user types being permitted.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.1
- CIS Controls v8 6.6
- NIST 800-53r5 CM-8, IA-8(2)

1.1.3 Requirement: Encrypt or hash all authentication credentials

Details: Ensure that local accounts and accounts with third parties use this approach to store your credentials. This will limit the impact of a third-party provider breach from impacting the technology. The encryption or hashing algorithm should be one approved for use by NIST.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.4
- CIS Controls v8 3.11
- NIST 800-53r5 IA-5(1)

1.1.4 Requirement: Customer administrators have access to an inventory of their user accounts

Details: Maintain an inventory of all accounts organized by authentication system. Maintain an up-to-date list of accounts for each system and tie each account to an individual person wherever possible. Having this ability in the platform helps organizations manage their users.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.6
- CIS Controls v8 5.3
- NIST 800-53r5 AC-2(3)

1.1.5 Requirement: Implement protections against brute force attacks

Details: Account lockout needs to be implemented to guard against brute forcing attacks against both the authentication and password reset functionality. After several tries on a specific user account, the account should be locked for a period of time or until unlocked by an administrative action or use of a separate authenticator controlled by the user. Additionally, it is best to continue the same failure message indicating that the credentials are incorrect or the account is locked to prevent an attacker from harvesting usernames.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.2.4
- NIST 800-53r5 AC-7

1.1.6 Requirement: Require multi-factor authentication for all administrative access

Details: Use multi-factor authentication (MFA) via encrypted channels for all administrative account access. Administrative accounts have tremendous capabilities to do harm if taken over through a social engineering or other attack. Protecting them with MFA is extremely important.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.4.5
- CIS Controls v8 6.5
- NIST 800-53r5 IA-2(1)

20.1.2 1.2 Maturity Level 2

1.2.1 Requirement: Implement a strong password reset system

Details: The password reset systems will leverage access to email or other known authenticators, such as confirming possession of a hardware token or a mobile device. Email alone should be augmented by security questions. When you do ask questions for password resetting, base them on questions that are both hard to guess, hard to brute force, and are not available through social media or previous data breaches. Additionally, any password reset option must not reveal whether an account is valid, preventing username harvesting.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.2.2

- NIST 800-53r5 IA-5(1)

1.2.2 Requirement: Block commonly used passwords

Details: When credentials are set up for a new account, those credentials are run against a list of commonly used password and password patterns to ensure that users are not using passwords that are easily guessable.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.4.4
- CIS Controls v8 5.2
- NIST 800-53r5 IA-5(1)

1.2.3 Requirement: Provide options for multi-factor authentication

Details: Allow users to protect their accounts with MFA. Allow users to choose the authenticator that works best for them, subject to meeting security requirements. Where possible, allow the issuance of multiple authenticators so that multiple combinations can still meet an MFA requirement and be used in the reissuance of lost or stolen authenticators.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.2.8
- NIST 800-53r5 IA-2(1)(2)

1.2.4 Requirement: Ensure authentication is centrally managed

Details: Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems. This makes it easier to ensure all users are being properly authenticated with the appropriate level of scrutiny and can centralize authentication logging as well.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.2
- CIS Controls v8 5.6
- NIST 800-53r5 IA-2(1)

1.2.5 Requirement: Provide capability to identify unassociated accounts

Details: Provide the ability for customer admins to identify and disable any account that cannot be associated with a business process or business owner. Try to document relevant business processes and owners to make auditing and maintaining accounts easier.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.8
- CIS Controls v8 5.3
- NIST 800-53r5 IA-2(3)

1.2.6 Requirement: Require multi-factor authentication

Details: Require MFA for all user accounts, on all systems, whether managed on-site or by a third-party provider. This is one of the best protections against social engineering attacks.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.3
- CIS Controls v8 6.3
- NIST 800-53r5 IA-2(1)(2)

20.1.3 1.3 Maturity Level 3

1.3.1 Requirement: Enable the integration with organization authentication systems

Details: By enabling customers to integrate their authentication system, such as Oauth and SAML, with the platform it makes it easier for them manage their users and ensure that users are maintained throughout the user life cycle.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.2
- CIS Controls v8 5.6
- NIST 800-53r5 IA-2(1)

1.3.2 Requirement: Automatically disable dormant accounts

Details: Automatically disable dormant accounts after a set period of inactivity. This is especially helpful for critical components of the technology and assist with the manual accounts audits that should be done on a periodic basis.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.9
- CIS Controls v8 5.3
- NIST 800-53r5 IA-2(3)

1.3.3 Requirement: Ensure temporary accounts have an expiration date

Details: Ensure that all temporary accounts have an expiration date that is monitored and enforced. This best practice should be applied to contractor accounts and accounts that are meant to be temporary. It is acceptable for service accounts and employee accounts to not have an expiration date. Treat users as temporary whenever there is uncertainty

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.10
- CIS Controls v8 5.3
- NIST 800-53r5 IA-2(3)

1.3.4 Requirement: Provide the ability for customer administrators to revoke access

Details: Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Employee new hire, termination, promotion, and demotion checklists should include the steps to setting user permissions commensurate with the employee's job responsibilities, or lack thereof. This should apply to employees and contractors.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.7
- CIS Controls v8 6.2
- NIST 800-53r5 IA-2(1)

1.3.5 Requirement: Allow password policy customization

Details: Allow customers to configure and enforce a strong password policy according to best practices - A password policy should be created and implemented so that passwords meet specific strength criteria.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.2.3
- NIST 800-53r5 IA-5(1)

1.3.6 Requirement: Authentication visibility

Details: Provide customers with visibility on user logins including the time, IP address of the login and user agents of the browser.

Applies to: All components

References

- N/A

20.2 2. Authorization Requirements

20.2.1 2.1 Maturity Level 1

2.1.1 Requirement: Platform provides an authorization system

Details: Platform provides an authorization system, such as Role Based Access Control (RBAC), that restricts access to sensitive data and functions - Protect all information stored on systems with file system, network share, claims, application, or database-specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.2.1
- CIS Controls v8 3.3
- NIST 800-53r5 AC-3, AC-5, AC-6, MP-2

2.1.2 Requirement: Applications and middleware should run with minimal privileges

Details: If an application becomes compromised, it is important that the application itself and any middleware services be configured to run with minimal privileges. For instance, while the application layer or business layer needs the ability to read and write data to the underlying database, administrative credentials that grant access to other databases or tables should not be provided.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.2.7
- NIST 800-53r5 AC-6, AC-6(8), SA-8(14)

2.1.3 Requirement: Apply the principle of least privilege

Details: Provide the customer with the ability to make all access decisions based on the principle of least privilege. Based on permission settings, access should be denied when not explicitly allowed. Additionally, after an account is created, rights must be specifically added to that account to grant access to resources. Where defaults are used, the defaults should be the minimal level of permissions.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.4.1
- NIST 800-53r5 AC-6, AC-6(8), SA-8(14)

2.1.4 Requirement: Use tokens to prevent forged requests

Details: In order to prevent Cross-Site Request Forgery (CSRF) attacks, you must embed a random value that is not known to third parties into the HTML form. This CSRF protection token must be unique to each request. This prevents a forged CSRF request from being submitted because the attacker does not know the value of the token.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.8
- NIST 800-53r5 AC-6, AC-6(8), SA-8(14)

20.2.2 Maturity Level 2

2.2.1 Requirement: Apply access controls checks consistently

Details: Always apply the principle of complete mediation, forcing all requests through a common security gatekeeper. This ensures that access control checks are triggered whether or not the user is authenticated.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.4.2
- NIST 800-53r5 AC-4

2.2.2 Requirement: Set the cookie domain and path correctly

Details: The cookie domain and path scope should be set to the most restrictive settings for your application. Any wildcard domain scoped cookie must have a good justification for its existence.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.5.1

2.2.3 Requirement: Verify object requests

Details: The product must verify during each request for data that the user has authorization to the data object. This prevents authenticated users from accessing data above or outside of their permission set.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.4.2
- NIST 800-53r5 AC-4(1)

2.2.4 Requirement: Apply the principle of separation of duties

Details: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions.

Applies to: All components

References

- CIS Controls V8 6.8
- NIST 800-53r5 AC-5

20.2.3 Maturity Level 3

2.3.1 Requirement: Do not use direct object references for access control checks

Details: Do not allow direct references to files or parameters that can be manipulated to grant excessive access. Access control decisions must be based on the authenticated user identity and trusted server-side information.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.4.4
- NIST 800-53r5 AC-4(1)

2.3.2 Requirement: Enforce access control to data through automated tools

Details: Use an automated tool, such as host-based data loss prevention, to enforce access controls to data even when the data is copied off a system.

> This will help ensure sensitive data that is not properly labeled is still protected from leaving its host system.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.2.9
- CIS Controls v8 13.3
- NIST 800-53r5 SI-4, SI-4(4)

2.3.3 Requirement: Restrict the use of shared and group accounts

Details: There are either no shared or group accounts or access to shared or group accounts is limited to a small number of trusted users.

Applies to: All components

References

- NIST 800-53r5 AC-2(9)

2.3.4 Requirement: Protection from data mining

Details: Data mining prevention and detection techniques include limiting the number and frequency of database queries to increase the work factor needed to determine the contents of databases, limiting types of responses provided to database queries, applying differential privacy techniques or homomorphic encryption, and notifying personnel when atypical database queries or accesses occur. Data mining protection focuses on protecting information from data mining while such information resides in organizational data stores.

Applies to: Web components

References

- NIST 800-53r5 AC-23

20.3 3. Boundary Protections Requirements

20.3.1 3.1 Maturity Level 1

3.1.1 Requirement: Deny communications with known malicious IP addresses

Details: Deny communications with known malicious or unused Internet IP addresses. Limit access to trusted and necessary IP address ranges at each of the organization's application and network boundaries. This can be done using a network firewall at the perimeter of your network. Preventing access from known malicious IP addresses can be done for all applications, even public facing ones. The Multi-State Infrastructure Information Sharing and Analysis Center (MS-ISAC) provides a list of known malicious IP addresses.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.1.3
- CIS Controls v8 9.2
- NIST 800-53r5 SI-8

3.1.2 Requirement: Deny communication over unauthorized ports

Details: Deny communication over unauthorized transportation control protocol (TCP) or user datagram protocol (UDP) ports or application traffic to ensure that only authorized protocols are allowed to cross each of the organization's network boundaries. System boundaries should be configured to deny traffic on all ports except ports explicitly needed for legitimate traffic.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.1.4
- CIS Controls v8 4.4, 4.5
- NIST 800-53r5 CA-9, SC-7, SC-7(5)

3.1.3 Requirement: Deploy network-based IDS sensors

Details: Deploy network-based intrusion detection systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries. Technology deployed outside of the jurisdictions' network should have a similar technology deployed and monitored.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.1.6
- CIS Controls v8 13.3
- NIST 800-53r5 SI-4, SI-4(4)

3.1.4 Requirement: Document traffic configuration rules

Details: All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need. This is important for production networks that host critical solutions. Exceptions are normal but should be few and must be removed when no longer necessary. This is one good reason to keep general purpose workstations in a separate network segment.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.3.2
- CIS Controls v8 4.4, 4.5
- NIST 800-53r5 CA-9, SC-7, SC-7(5)

3.1.5 Requirement: Use MFA for managing network infrastructure

Details: Manage network infrastructure using multi-factor authentication and encrypted sessions.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.3.5
- CIS Controls v8 12.3
- NIST 800-53r5 CM-6,CM-7, SC-23

3.1.6 Requirement: Configure perimeter devices to prevent common types of attacks

Details: Define strict “TCP keepalive” and “maximum connection” on all perimeter devices, such as firewalls and proxy servers. This assists with preventing the success of SYN Flood attacks. Another approach is leveraging SYN cookies to prevent TCP SYN floods. A SYN Flood is one of the most common forms of DDoS attacks observed by the MS-ISAC.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.5.4

3.1.7 Requirement: Disable wireless access on devices if it is not required

Details: Disable wireless access on devices that do not have a business purpose for wireless access. Periodically review device settings to ensure wireless options (Wi-Fi, Bluetooth, etc.) remain off.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.6.4
- CIS Controls v8 4.8
- NIST 800-53r5 CM-6, CM-7

3.1.8 Requirement: Documentation clearly identifies wireless capabilities

Details: Product documentation clearly defines any required wireless capability associated with the product along with information regarding the security and management of those wireless capabilities. Identify parts of the product that use a wireless connection, and document each access point. For Wi-Fi, this will be a Wi-Fi router and any endpoint devices. For Bluetooth and NFC, this may be multiple devices. The decision to enable wireless technology should be made by the system administrator using a risk-based decision-making process.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.6.1
- CIS Controls v81.1
- NIST 800-53r5 CM-8, CM-8(1), PM-5

3.1.9 Requirement: Provide dedicated wireless networks

Details: Create a separate wireless network for each separate use. Access from the wireless network should be treated as untrusted and filtered and audited accordingly. Use of any wireless technology in solutions should be isolated for a very specific purpose, and incoming connections from the wireless network should be handled with care.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.6.10
- CIS Controls v8 12.2
- NIST 800-53r5 CM-7, CP-6, CP-7, PL-8, PM-7, SA-6, SC-7

3.1.10 Requirement: Disable wireless peripheral access to devices

Details: Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose. Printers and other peripherals often have Bluetooth capabilities.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.6.9
- CIS Controls v8 4.8
- NIST 800-53r5 CM-6, CM-7

20.3.2 3.2 Maturity Level 2

3.2.1 Requirement: Enable firewall logging

Details: Enable firewall logging of accepted and denied traffic to determine where a DDoS may be originating from. Most technology must be careful not to block based on IP address unless there is evidence of malicious behavior.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.5.3
- CIS Controls v8 8.2
- NIST 800-53r5 AU-2, AU-7, AU-12

3.2.2 Requirement: Configure devices to detect and alarm on traffic anomalies

Details: Configure firewalls and intrusion detection/prevention devices to alarm on traffic anomalies. Establish and regularly validate baseline traffic patterns (volume and type) for public-facing websites. Active and automated monitoring during peak periods is critical to early detection and mitigation of DDoS attacks.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.5.5
- CIS Controls v8 13.6
- NIST 800-53r5 SI-4, SI-4(4)

3.2.3 Requirement: Limit wireless access on client devices to only authorized wireless networks

Details: Configure wireless access only on client machines that have an essential wireless business purpose. Allow access only to authorized wireless networks, and restrict access to other wireless networks. All Wi-Fi connected technology devices must only connect to the authorized wireless access point and no other.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.6.5
- CIS Controls v8 12.6
- NIST 800-53r5 AC-18

3.2.4 Requirement: Disable peer-to-peer wireless network capabilities on wireless clients

Details: Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.6.6
- CIS Controls v8 12.6
- NIST 800-53r5 AC-18, SC-23

3.2.5 Requirement: Segment the network based on sensitivity

Details: Segment the network based on the label or classification level of the information stored on the servers, and locate all sensitive information on separated Virtual Local Area Networks (VLANs). Consider establishing unique networks for each critical technology and service offering.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.2.5
- CIS Controls v8 3.12
- NIST 800-53r5 SC-7, SC-7(13)

3.2.6 Requirement: Apply upstream port and packet size filtering

Details: Have upstream network service provider or network appliance apply port and packet size filtering to limit unnecessary traffic to the product's network infrastructure. Work with upstream providers to filter out as much as possible that is not related to the service being provided.

Applies to: Hosted Components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.5.2

20.3.3 3.3 Maturity Level 3

3.3.1 Requirement: Deploy network-based intrusion prevention systems

Details: Deploy network-based intrusion prevention systems (IPS) to block malicious network traffic at each of the organization's network boundaries. This should be applied to all network-connected technology. It must be monitored and configured to ensure it does not prevent legitimate traffic.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.1.7

- CIS Controls v8 13.8
- NIST 800-53r5 SI-4, SI-4(4)

3.3.2 Requirement: Manage all vendor-issued devices remotely accessing sensitive networks

Details: Scan all vendor issued devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.1.12
- CIS Controls v8 13.5
- NIST 800-53r5 AC-17, AC-17(1), SC-7, SI-4

3.3.3 Requirement: Manage system's external removable media's read/write configurations

Details: Configure systems not to write data to external removable media, if there is no business need for supporting such devices. This prevents someone with physical access to a system storing sensitive information from extracting that information onto a USB drive.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.1.7
- NIST 800-53r5 SC-34(1)

3.3.4 Requirement: Limit workstation-to-workstation communication

Details: When not in use, limit workstation-to-workstation communication using technologies such as private VLANs or micro-segmentation. Whenever possible, workstations should be limited to talking only to servers thereby limiting lateral movement between workstations.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.2.7
- CIS Controls v8 4.1
- NIST 800-53r5 CM-1, CM-2, CM-6, CM-7, CM-7(1), CM-9, SA-3, SA-8, SA-10

3.3.5 Requirement: Use wireless authentication protocols that require mutual, multi-factor authentication

Details: Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS) that requires mutual, multi-factor authentication. Use of wireless technology in solutions demands that all parties be properly and fully authenticated.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.6.8
- CIS Controls v8 12.6
- NIST 800-53r5 AC-18, SC-23

3.3.6 Requirement: Limit access to trusted IP address ranges

Details: By applying an allowlist of known trusted IP addresses this allows organizations to greatly reduce their attack surface. This can be done using a network firewall at the perimeter of your network. Preventing access from known malicious IP addresses can be done for all applications, even public facing ones. The Multi-State Infrastructure Information Sharing and Analysis Center (MS-ISAC) provides a list of known malicious IP addresses.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.1.3
- CIS Controls v8 9.2
- NIST 800-53r5 SI-8

20.4 4. Data Confidentiality and Integrity Requirements

20.4.1 4.1 Maturity Level 1

4.1.1 Requirement: Use valid HTTPS certificates from a reputable certificate authority

Details: HTTPS certificates should be signed by a reputable certificate authority (CA). The name on the certificate should match the fully qualified domain name (FQDN) of the website. The certificate itself should be valid and not expired.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.1.2
- NIST 800-53r5 IA-5(2)

4.1.2 Requirement: Encrypt transmittal of username and authentication credentials

Details: Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. This includes network traffic and data moved using removable media.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.5
- CIS Controls v8 3.10
- NIST 800-53r5 AC-17(2), IA-5, IA-5(1), SC-8, SC-8(1)

4.1.3 Requirement: Use the Strict-Transport-Security header

Details: The Strict-Transport-Security header ensures that the browser does not talk to the server over non-TLS. This helps reduce the risk of TLS stripping attacks as implemented by the TLSsniff tool.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.1.10

4.1.4 Requirement: Disable data caching using cache control headers and autocomplete

Details: Browser data caching should be disabled using the cache control HTTP headers or meta tags within the hypertext markup language (HTML) page. Additionally, sensitive input fields, such as the login form, should have the autocomplete=off setting in the HTML form to instruct the browser not to cache the credentials.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.1.3

4.1.5 Requirement: Updated TLS configuration on servers

Details: Weak ciphers must be disabled on all servers. For example, SSL v2, SSL v3, and TLS protocols prior to v1.2 have known weaknesses and are not considered secure. Additionally, disable the NULL, RC4, DES, and MD5 cipher suites. Ensure all key lengths are greater than 128 bits, use secure renegotiation, and disable compression.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.1.5

4.1.6 Requirement: Use TLS everywhere

Details: TLS should be used whenever data is transferred over a network. TLS must be applied to any authentication pages as well as all pages after the user is authenticated. If sensitive information (e.g., personal information) can be submitted before authentication, those features must also be sent over TLS.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.1.6
- CIS Controls v8 3.10
- NIST 800-53r5 AC-17(2), IA-5, IA-5(1), SC-8, SC-8(1)

4.1.7 Requirement: Disable HTTP access for all TLS-enabled resources

Details: For all pages requiring protection by TLS, the same URL should not be accessible via the non-TLS channel.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.1.9

4.1.8 Requirement: Do not disclose too much information in error messages

Details: Messages for authentication errors must be clear and, at the same time, must be written so that sensitive information about the system is not disclosed. For example, error messages that reveal that the userid is valid but that the corresponding password is incorrect confirms to an attacker that the account does exist on the system. Instead, provide only a message that indicates that the login failed.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.2.5

4.1.9 Requirement: Display generic error messages

Details: Error messages should not reveal details about the internal state of the application. For example, file system path and stack information should not be exposed to the user through error messages.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.6.1

4.1.10 Requirement: Store user passwords using a strong, iterative, salted hash

Details: User passwords must be stored using secure hashing techniques with strong algorithms like PBKDF2, bcrypt, or SHA-512. Simply hashing the password a single time does not sufficiently protect the password. Use adaptive hashing (a work factor) combined with a randomly generated salt for each user to make the hash strong.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.1.8
- CIS Controls v8 3.11
- NIST 800-53r5 IA-5(1), SC-28, SC-28(1)

20.4.2 4.2 Maturity Level 2

4.2.1 Requirement: Encrypt the hard drive of all vendor-issued devices

Details: Utilize approved whole disk encryption software to encrypt the hard drive of all devices issued by the vendor. Determine what sensitive information you will permit on employees' laptops and mobile devices. Ensure the hard drives of laptops and mobile devices are fully encrypted to prevent information from being stolen.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.1.5
- CIS Controls v8 3.6

- NIST 800-53r5 SC-28

4.2.2 Requirement: Encrypt data on USB storage devices

Details: If USB storage devices are required, all data stored on such devices must be encrypted while at rest.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.1.8
- CIS Controls v8 3.6
- NIST 800-53r5 SC-28

4.2.3 Requirement: Encrypt all sensitive information in transit

Details: Encrypt all sensitive information in transit. Consider whether the data's confidentiality is sensitive. If you are unsure, consider it sensitive.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.2.3
- CIS Controls v8 3.10
- NIST 800-53r5 AC-17(2), IA-5, IA-5(1), SC-8, SC-8(1)

4.2.4 Requirement: Encrypt sensitive information at rest

Details: Encrypt all sensitive information at rest. Databases and their backups, for example, should be encrypted to ensure they are protected from manipulation.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.2.4
- CIS Controls v8 3.11
- NIST 800-53r5 IA-5(1), SC-28, SC-28(1)

4.2.5 Requirement: Leverage the Advanced Encryption Standard (AES) to encrypt wireless data

Details: Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit. Wi-Fi, Bluetooth, and NFC all support encrypted communication. Ensure Wi-Fi uses Wi-Fi Protected Access 2 (WPA2) or better.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.6.7
- CIS Controls v8 3.10
- NIST 800-53r5 AC-17(2), IA-5, IA-5(1), SC-8, SC-8(1)

4.2.6 Requirement: Limit the use and storage of sensitive data

Details: Product ensures that sensitive data is not being unnecessarily transported or stored. Where possible, use tokenization to reduce data exposure risks.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.1.1

4.2.7 Requirement: Do not use unvalidated forwards or redirects

Details: An unvalidated forward can allow an attacker to access private content without authentication. Unvalidated redirects allow an attacker to lure victims into visiting malicious sites. Prevent these from occurring by conducting the appropriate access control checks before sending the user to the given location.

Applies to: Web Components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.4.3

4.2.8 Requirement: Follow secure configuration guidance for cloud storage

Details: Follow guidance from CIS Foundations Benchmarks or other secure configuration guidance to ensure all cloud storage containers with sensitive data are properly secured. CIS Foundations Benchmarks are available for Amazon Web Services, Microsoft Azure, Google Cloud, and Microsoft 365.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.3.1
- CIS Controls v8 4.1
- NIST 800-53r5 CM-1, CM-2, CM-6, CM-7, CM-7(1), CM-9, SA-3, SA-8, SA-10

4.2.9 Requirement: Use only standardized and extensively reviewed encryption algorithms

Details: Use only standardized and extensively reviewed encryption algorithms that are validated by trusted third parties, such as NIST. Use standard libraries available from reputable sources instead of developing your own cryptographic solutions.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 3.2.15
- CIS Controls v8 16.11
- NIST 800-53r5 SA-15

20.4.3 4.3 Maturity Level 3

4.3.1 Requirement: Monitor and block unauthorized movement of sensitive data

Details: Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security personnel. Deploy and configure Data Loss Prevention (DLP) solutions to look for sensitive information that should not be leaving your network boundaries.

Applies to: All Components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.1.3
- CIS Controls v8 3.13
- NIST 800-53r5 CA-7, CM-12, CM-12(1), SC-4

4.3.2 Requirement: Utilize an active discovery tool to identify sensitive data

Details: Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory. This helps an organization find and secure all instances of sensitive information.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.2.8
- CIS Controls v8 3.13
- NIST 800-53r5 CA-7, CM-12, CM-12(1), SC-4

4.3.3 Requirement: Digitally sign sensitive information in transit

Details: Sensitive data should be digitally signed by its originator and verified by all components which read, store, or process the data. The integrity of the data must be maintained throughout its lifecycle.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.2.2
- NIST 800-53r5 SC-8(1)

4.3.4 Requirement: Encrypt data stored in cloud storage containers

Details: Use application encryption with secret keys only known to the data owner(s) to protect confidential data stored in a cloud storage container.

> This protects the data even in the event of a data breach of the cloud hosting provider or a misconfiguration of the cloud storage container's permissions.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.3.2
- CIS Controls v8 3.11
- NIST 800-53r5 IA-5(1), SC-28, SC-28(1)

4.3.5 Requirement: Use separate storage containers for unique data classifications

Details: Don't overload one container with data at various classification levels. Create separate containers with appropriate names and configuration settings for each data classification level. Follow your data classification scheme and establish containers based on sensitivity. Also, don't mix production and test data.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.3.4
- CIS Controls v8 3.12
- NIST 800-53r5 SC-4

4.3.6 Requirement: Remove or isolate sensitive data or systems not regularly accessed by the organization

Details: Remove sensitive data or systems not regularly accessed by the organization from the network. These systems should only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed. In addition, disconnect systems that store or process data that do not absolutely have to be online. Do not leave USB devices with sensitive information plugged into machines when they are not in use.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.1.2
- CIS Controls v8 3.5
- NIST 800-53r5 MP-6

20.5 5. System Availability Requirements

20.5.1 5.1 Maturity Level 1

5.1.1 Requirement: Ensure regular automated backups

Details: Ensure that all system data is automatically backed up on a regular basis.

> Backups of data should be done on a nightly basis. There may be applications which need to back up data at even higher frequencies during critical periods.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.4.1
- CIS Controls v8 11.2
- NIST 800-53r5 CP-8, CP-9

5.1.2 Requirement: Backup data should be restorable

Details: Verify backup data is restorable by performing a data restoration.

This is important to do frequently for some systems.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.4.3
- CIS Controls v8 11.5
- NIST 800-53r5 CP-4, CP-9(1)

5.1.3 Requirement: Local distributed storage capability

Details: Ensure data storage components have local fail over options in the event of a service degradation for primary component.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.4.3
- CIS Controls v8 11.4
- NIST 800-53r5 CP-6

5.1.4 Requirement: Local distributed processing capability

Details: Ensure application components have local fail over options in the event of a service degradation for primary component.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.4.3
- CIS Controls v8 12.2
- NIST 800-53r5 CP-7

20.5.2 5.2 Maturity Level 2

5.2.1 Requirement: Perform complete system backups

Details: Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system. On premises

products must provide this capability. These types of backups should be done frequently for each type of system used. This allows for quick recovery back to the known good version. Maintaining extra units created from these system backups is another good approach.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.4.2
- CIS Controls v8 11.2
- NIST 800-53r5 CP-9, CP-10

5.2.2 Requirement: Remote distributed storage capability

Details: Ensure data storage components have fail over options in separate geographic regions in the event of a service degradation for primary component.

This is important to do frequently for some systems.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.4.3
- CIS Controls v8 11.4
- NIST 800-53r5 CP-6

5.2.3 Requirement: Remote distributed processing capability

Details: Ensure application components have fail over options in separate geographic regions in the event of a service degradation for primary component.

This is important to do frequently for some systems.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.4.3
- CIS Controls v8 12.2
- NIST 800-53r5 CP-7

20.5.3 5.3 Maturity Level 3

5.3.1 Requirement: Establish DDoS mitigation services with a third-party DDoS mitigation provider

Details: Obtain third-party DDoS mitigation services. Whether free or at a cost, these services can be very helpful to protect the most critical internet-connected functions.

Applies to: Hosted components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.5.6
- CIS Controls v8 12.2
- NIST 800-53r5 SC-5, SC-5(1), SC-5(2)

5.3.2 Requirement: Fail in a known state

Details: When a system fails in a known state, it safeguards the confidentiality, integrity, or availability of data, even in the event of faults in organizational systems or their components. By maintaining system state information, the restart of the system and its return to operational mode can occur with minimal disruption to mission-critical and business processes.

Applies to: All components

References

- NIST 800-53r5 SC-24

5.3.3 Requirement: No single points of failure

Details: The system should be designed in a manner that does not contain a single point of failure that could bring down the entire system.

Applies to: All components

References

- CIS Controls v8 12.2
- NIST 800-53r5 SA-8

20.6 6. Injection Prevention Requirements

In these requirements, *interpreted* is defined as: Input that may be treated as data or as code depending on its content.

20.6.1 6.1 Maturity Level 1

6.1.1 Requirement: Use secure HTTP response headers

[Public key pins is deprecated. Unclear if replacement is well supported]

Details: To protect against cross-site scripting (XSS) and man-in-the-middle (MITM) attacks, use the Content Security Policy (CSP) and Public-Key-Pins headers.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.2

6.1.2 Requirement: Validate uploaded files

Details: When accepting file uploads from the user, make sure to validate the size of the file, the file type, and the file contents as well as ensure that it is not possible to override the destination path for the file.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.6

6.1.3 Requirement: Set the encoding for your application

Details: For every page in your application, set the encoding using HTTP headers or meta tags within HTML. This ensures that the encoding of the page is always defined and that the browser will not have to determine the encoding on its own. Setting a consistent encoding, like Unicode transformation format 8 bit (UTF-8), for your application reduces the overall risk of issues like XSS.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.7

6.1.4 Requirement: Validate all input

Details: For each user input field, there should be validation on the input content.

> Examples of validation include data type validation, length validation, pattern validation, among others.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.10
- CIS Controls v8 16.10
- NIST 800-53r5 PL-8, SA-8, SI-10, SI-10(6)

20.6.2 6.2 Maturity Level 2

6.2.1 Requirement: Use parameterized inputs

Details: Input to an interpreter (e.g. an SQL Engine) should be passed using parameterized input, such as a bind variable. If Dynamic SQL is constructed within stored procedures, the procedural database code must also use bind variables. For example `dbms_sql` (Oracle), `EXECUTE IMMEDIATE` (Oracle) and `execute sp_executesql` (SQL Server) allow dynamic SQL to be constructed from within stored procedures or triggers. Satisfies: Prefer Whitelists Over Blacklists for Input Validation

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.9

6.2.2 Requirement: Use the X-Frame-Options header

Details: Use the X-Frame-Options header to prevent content from being loaded by a foreign site in a frame. This mitigates Clickjacking attacks. For older browsers that do not support this header, add frame busting JavaScript code to mitigate Clickjacking (although this method is not foolproof and can be circumvented). The use of frame busting is only required for products that support browsers that do not support X-Frame-Options.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.1

6.2.3 Requirement: Use the nosniff header for uploaded content

Details: When hosting user uploaded content that can be viewed by other users, use the X-Content-Type-Options: nosniff header so that browsers do not try to guess the data type. Sometimes the browser can be tricked into displaying the data type incorrectly (e.g., showing a GIF file as HTML). Always let the server or application determine the data type.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.3

6.2.4 Requirement: Conduct contextual output encoding

Details: All output functions must contextually encode data before sending it to the user. Depending on where the output will end up in the HTML page, the output must be encoded differently. For example, data placed in the URL context must be encoded different than data placed in JavaScript context within the HTML page.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.5

20.6.3 6.3 Maturity Level 3

6.3.1 Requirement: Deploy web application firewalls (WAFs)

Details: Protect web applications by deploying WAFs that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 3.2.14
- CIS Controls v8 13.10
- NIST 800-53r5 SC-7(8)

6.3.2 Requirement: Use allowlist on interpreted input

Details: For input that will be interpreted, allowlist acceptable inputs. Only inputs that appear on the whitelist will be accepted.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.10

6.3.3 Requirement: Validate the source of input

Details: The HTTP method used to make a request must be validated. For example, if input is expected from a POST request, do not accept the input variable from a GET request.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.3.4

20.7 7. Logging/Alerting Requirements

20.7.1 7.1 Maturity Level 1

7.1.1 Requirement: Activate audit logging

Details: Ensure that logging has been enabled on all systems and networking devices. Components of technology solutions must utilize available logging capabilities to store system activity.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.3.1
- CIS Controls v8 8.2
- NIST 800-53r5 AU-2, AU-7, AU-12

7.1.2 Requirement: Ensure adequate storage for logs

Details: The product must provide a mechanism to maintain the storage of logs over a certain period of time. Logs should be retained for a minimum of 180 days with the option to archive logs for longer periods of time.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.3.2
- CIS Controls v8 8.3
- NIST 800-53r5 AU-4

7.1.3 Requirement: Log all authentication activities

Details: Log all authentication activities, whether successful or not.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.6.4
- CIS Controls v8 8.12
- NIST 800-53r5 AU-2

7.1.4 Requirement: Log all privilege changes

Details: Log all activities or occasions where the user's privilege level escalates.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.6.5
- CIS Controls v8 8.12
- NIST 800-53r5 AU-2

7.1.5 Requirement: Do not log inappropriate data

Details: While logging errors and auditing access is important, sensitive data must never be logged in an unencrypted form. For example, under HIPAA and PCI, it would be a violation to log sensitive data into the log itself unless the log is encrypted on the disk. Additionally, it can create a serious exposure point should the application itself become compromised.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.6.8

7.1.6 Requirement: Store logs securely

Details: Logs must be stored and maintained appropriately to avoid information loss or tampering by an intruder. Log retention should also follow the retention policy set forth by the organization to meet regulatory requirements and provide enough information for forensic and incident response activities.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.6.9
- CIS Controls v8 8.10
- NIST 800-53r5 AU-9, AU-11

7.1.7 Requirement: Log and alert on changes to administrative group membership

Details: Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges. Changes to technology administrator accounts must be logged and alerted. Quick notification allows for timely remediation in the event of privilege escalation or other attack.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.4.8
- CIS Controls v8 8.5
- NIST 800-53r5 AU-3, AU-3(1), AU-7, AU-12

20.7.2 7.2 Maturity Level 2

7.2.1 Requirement: Alerting

Details: Provide a mechanism to alert responsible parties to the occurrence of certain logged events. The method of alerting can vary, but must take the form of a “push” notification.

Applies to: All components

References

- NIST 800-53r5 AU-5, AU-5(2)

7.2.2 Requirement: Centralize anti-malware logging

Details: The product must allow all malware detection events to be sent to enterprise anti-malware administration tools and event log servers for analysis and alerting. This assists in the early detection of an incident and ensures the proper security personnel are alerted to malware on the network.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.3.4
- CIS Controls v8 8.2
- NIST 800-53r5 AU-2, AU-7, AU-12

7.2.3 Requirement: Enable DNS query logging

Details: Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains. This is used to detect attempts to reach known malicious sites from within your network. This will help detect malware and prevent it from communicating with its command and control infrastructure.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.3.5
- CIS Controls v8 8.2
- NIST 800-53r5 AU-2

7.2.4 Requirement: Enable command-line audit logging

Details: Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash. A large percentage of malware uses Powershell and Bash. This logging will assist in the detection of malware and a better understanding of its impact.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.3.6
- CIS Controls v8 8.8
- NIST 800-53r5 AU-2

7.2.5 Requirement: Enable detailed logging

Details: Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. Technology components particularly servers and those devices in publicly accessible network interfaces should capture detailed enough information to fully understand and reconstruct security incidents.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.3.6
- CIS Controls v8 8.5
- NIST 800-53r5 AU-3, AU-3(1), AU-7, AU-12

7.2.6 Requirement: Log user activity

Details: Log relevant use activity, at a minimum login times, pages/screens viewed. Take care to not log information that would violate voter or ballot privacy. This can greatly assist with understanding the impact of security incidents involving user accounts. This is especially important for administrators.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.6.10
- CIS Controls v8 8.2
- NIST 800-53r5 AU-2

7.2.7 Requirement: Log administrative activities

Details: Log all administrative activities on the application or any of its components.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.6.6
- CIS Controls v8 8.2
- NIST 800-53r5 AU-2

20.7.3 7.3 Maturity Level 3

7.3.1 Requirement: Log and alert on unsuccessful administrative account login

Details: Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account. This enables technology administrators to detect attempts to brute force or socially engineer access to administrator accounts.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.4.9

- CIS Controls v8 8.5
- NIST 800-53r5 AU-3, AU-3(1), AU-7, AU-12

7.3.2 Requirement: Enforce detail logging for access or changes to critical or sensitive data

Details: Enforce detailed audit logging for access to sensitive data or changes to sensitive data using tools such as file integrity monitoring or security information and event monitoring. This can help detect a malicious attempt to alter the integrity of the data. Database level logging can be enabled to track all changes to the database.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 4.2.10
- CIS Controls v8 3.14
- NIST 800-53r5 AC-6(9), AU-2, AU-12

7.3.3 Requirement: Monitor attempts to access deactivated accounts

Details: Monitor attempts to access deactivated accounts through audit logging. This can alert system administrators to likely malicious behavior.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.12
- CIS Controls v8 8.5
- NIST 800-53r5 AU-3, AU-3(1), AU-7, AU-12

7.3.4 Requirement: Alert on account login behavior deviation

Details: Alert when users deviate from normal login behavior, such as time-of-day, workstation location, and duration.

> Major commercial systems have the capability to establish an activity baseline based on time of day, IP address, and other data. Where possible, set up alerts to anomalous behavior for early detection of a possible attack.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.13

- CIS Controls v8 8.5
- NIST 800-53r5 AU-3, AU-3(1), AU-7, AU-12

7.3.5 Requirement: Deploy SIEM or log analytic tools

Details: Support the use of Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.

> Timely and accurate detection of potential security events is critical during peak periods. A SIEM solution can greatly assist with this.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.3.4
- CIS Controls v8 13.1
- NIST 800-53r5 AU-6(1), AU-7, IR-4(1), SI-4(2), SI-4(5)

7.3.6 Requirement: Log access to sensitive data

Details: Log all access to sensitive data. This is particularly important for corporations that have to meet regulatory requirements like Health Insurance Portability and Accountability Act (HIPAA), PCI, or Sarbanes-Oxley Act (SOX).

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.6.7
- CIS Controls v8 8.5
- NIST 800-53r5 AU-3, AU-3(1), AU-7, AU-12

7.3.7 Requirement: Central log management

Details: Logs must be aggregated to a central log management system for analysis and review. Networked technology solutions must utilize central event logging. Central event logging is extremely beneficial for detecting events and ensuring event logs are properly protected.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.3.5

- CIS Controls v8 8.9
- NIST 800-53r5 AU-6(3)

20.8 8. Secret Management Requirements

20.8.1 8.1 Maturity Level 1

8.1.1 Requirement: Do not hardcode credentials

Details: Never allow credentials to be stored directly within the application code. While it can be convenient to test the application code with hardcoded credentials during development, this significantly increases risk and should be avoided.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.2.1
- NIST 800-53r5 IA-5(7)

8.1.2 Requirement: Store credentials securely

Details: Modern web applications usually consist of multiple layers. The business logic tier often connects to the other tiers, such as a database. Connecting to a database, of course, requires authentication. The authentication credentials, if stored, must be stored in a centralized location that is under strict access control. Scattering credentials throughout the source code is not acceptable. Some development frameworks provide a centralized secure location for storing credentials. These encrypted stores should be leveraged when possible.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.2.6
- NIST 800-53r5 IA-5(6)

8.1.3 Requirement: Credentials for non-production and production environments are different

Details: Credentials for non-production environments must be different from production environment credentials and secrets.

Applies to: All components

References

- CIS Controls v8 5.2
- NIST 800-53r5 IA-5

20.8.2 8.2 Maturity Level 2

8.2.1 Requirement: Set up secure key generation processes

Details: When keys are generated and stored in your system, the product must use PKCS standards and provide a way for customers to securely generate those keys to provide mutual authentication and non-repudiation between components.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.1.4
- NIST 800-53r5 SC-12(2), SC-12(3)

8.2.2 Requirement: Securely exchange encryption keys

Details: If encryption keys are exchanged or preset in your application, any key establishment or exchange must be performed over a secure channel.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.1.7
- NIST 800-53r5 SC-12(2), SC-12(3)

8.2.3 Requirement: Developers are not allowed to access production credentials

Details: Production credentials and secrets should be managed outside of the development team on a need to know basis and injected into the application at runtime whenever feasible.

Applies to: All components

References

- CIS Controls v8 5.2
- NIST 800-53r5 IA-5

20.8.3 8.3 Maturity Level 3

8.3.1 Requirement: Use hardware security modules or key management service for keys

Details: Use a Hardware Security Module (HSM) or Key Management Service (KMS) when using cryptographic keys. These products are tamper evident and provide a secure environment for the management and operation of keys.

Applies to: All components

References

- NIST 800-53r5 SC-12(2), SC-12(3)

8.3.2 Requirement: Use a FIPS 140-3 validated module

Details: Use a cryptographic module that meets or exceeds FIPS 140-2 validation, operating in FIPS mode, for performing cryptographic operations. It is only necessary that the cryptographic software is FIPS 140-2 (or newer) certified, not the specific hardware.

Applies to: All components

References

- NIST Voluntary Voting System Guideline Requirements Version 2.0 (Draft) 13.3-A
- NIST 800-53r5 SC-12(2), SC-12(3)

20.9 9. System Integrity Requirements

20.9.1 9.1 Maturity Level 1

9.1.1 Requirement: Install the latest stable version of any security-related updates on all network devices

Details: Install the latest stable version of any security-related updates on all network devices. Latest refers to all updates which were available prior to the internal product testing of the product. Ensure that you are monitoring for updates. The vendor must use the most recent security updates available at the beginning of the development cycle, or later.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 1.3.4
- CIS Controls v8 7.4, 12.1
- NIST 800-53r5 RA-5, RA-7, SI-2, SI-2(2), CM-8(1)

9.1.2 Requirement: Ensure anti-malware software and signatures are updated

Details: For systems that support the use of anti-malware software, the product must allow an administrator to perform updates to its scanning engine and signature database. Ensure that all anti-malware instances are receiving signature updates. This requires periodic review of devices within the technology system.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.3.2
- CIS Controls v8 10.2
- NIST 800-53r5 SI-3

9.1.3 Requirement: Configure devices to not auto-run content

Details: Configure devices to not auto-run executable code from removable media. This helps ensure an attacker cannot insert a malicious device and execute it without having user credentials.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.5.3
- CIS Controls v8 10.3
- NIST 800-53r5 MP-7

9.1.4 Requirement: Use port protectors on unused ports

Details: Cover all unused communication ports (e.g. USB, Thunderbolt, HDMI, etc.) on endpoint devices with locks or tamper-evident port protectors to ensure unauthorized devices are not inserted into the device. This must be done prior to delivery to the customer.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.5.6
- NIST 800-53r5 CM-7

9.1.5 Requirement: Configure anti-malware scanning of removable devices

Details: Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected. Use of USB devices is very common in certain systems. Therefore, it is critical that all external devices be scanned for malware prior to use.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.5.5
- CIS Controls v8 10.4
- NIST 800-53r5 MP-7, SI-3

20.9.2 9.2 Maturity Level 2

9.2.1 Requirement: Deploy operating system patches

Details: Ensure operating systems are running the latest security updates provided by the software vendor. Latest refers to all updates which were available prior to the internal product testing of the product.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.2.4
- CIS Controls v8 7.3
- NIST 800-53r5 RA-5, RA-7, SI-2, SI-2(2)

9.2.2 Requirement: Deploy software patches

Details: Ensure that third-party software on all systems is running the latest security updates provided by the software vendor. Latest refers to all updates which were available prior to the internal product testing of the product.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.2.5
- CIS Controls v8 7.4
- NIST 800-53r5 RA-5, RA-7, SI-2, SI-2(2)

9.2.3 Requirement: Utilize centrally managed anti-malware software

Details: Utilize centrally managed anti-malware software to continuously monitor and defend workstations and servers. All endpoints in an technology solution must use properly installed and constantly running anti-malware software. Central management allows administrators to enforce this rule.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.3.1
- CIS Controls v8 10.6
- NIST 800-53r5 SI-3

9.2.4 Requirement: Limit access to scripting tools

Details: Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities. Technology may make use of these technologies, but access to them should be limited to only the most trusted and protected accounts.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.4.7
- CIS Controls v8 2.7
- NIST 800-53r5 CM-7, CM-7(1), SI-7, SI-7(1)

9.2.5 Requirement: Use standard hardening configuration templates for databases

Details: For applications that rely on a database, use standard hardening configuration templates. CIS Benchmarks are available for various database offerings such as MySQL, SQL Server, and PostgreSQL. Guidance for cloud-based databases are also available.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 3.2.16
- CIS Controls v8 16.7
- NIST 800-53r5 CM-6, CM-7

9.2.6 Requirement: Establish secure configurations

Details: Maintain documented, standard security configuration standards for all authorized operating systems and software such as the CIS Benchmarks. Using a vetted configuration standard, identify each component of the technology and its secure configuration standard to use.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.1.1
- CIS Controls v8 4.1
- NIST 800-53r5 CM-1, CM-2, CM-6, CM-7, CM-7(1), CM-9, SA-3, SA-8, SA-10

20.9.3 9.3 Maturity Level 3

9.3.1 Requirement: Implement automated configuration monitoring systems

Details: Utilize a Security Content Automation Protocol (SCAP) compliant or equivalent configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur. This prevents accidental misconfiguration and allows RTPs the ability to prove the component has been properly and securely configured.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.1.4
- CIS Controls v8 16.7
- NIST 800-53r5 CM-6

9.3.2 Requirement: Deploy system configuration management tools

Details: Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. Where possible, each component should be inspected and updated with the latest known good secure configuration prior to use.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.1.5
- CIS Controls v8 4.1

- NIST 800-53r5 CM-9, SA-10

9.3.3 Requirement: Enable operating system anti-exploitation features and deploy anti-exploit technologies

Details: Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system, or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. This applies to servers and other sensitive endpoints.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.3.3
- CIS Controls v8 10.5
- NIST 800-53r5 SI-16

9.3.4 Requirement: Disable access to USB devices where possible

Details: Disable the use of USB devices (including Thunderbolt) on a system. This completely removes the risk of removable USB media based attacks. This may not be feasible for all components. It should be feasible for servers and other devices which do not use USB connected devices.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.5.7

9.3.5 Requirement: Use USB Write Blockers to transfer data into sensitive systems

Details: Use USB Write Blockers to allow a high integrity system to read the content of a USB device. This mitigates the risk of transferring any malicious payload. These devices should be used when transferring data into sensitive systems using removable USB media.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 2.5.8

9.3.6 Requirement: Deny application execution by default

Details: Implement default-deny technologies (such as AppLocker) to only permit applications on an allow-list to execute on the product. An allow-list of acceptable applications should be established by the vendor based on the use-cases of the application.

Applies to: All components

References

- CIS Controls v8 2.5
- NIST 800-53r5 CM-7(5), CM-10

20.10 10. User Session Management Requirements

20.10.1 10.1 Maturity Level 1

10.1.1 Requirement: Set the cookie expiration time

Details: Set the session cookie expiration time to a reasonable value given the sensitivity of the data. Non-expiring session cookies should only be allowed for applications with no sensitive information, such as one providing basic public information that is customized for a user.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.5.2

10.1.2 Requirement: Place a logout button on every page

Details: Place the logout button or logout link in an easily accessible place for every authenticated page.

Scope: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.5.3

10.1.3 Requirement: Use secure cookie attributes (i.e., HttpOnly and Secure Flags)

Details: Set the session cookie with both the HttpOnly and Secure flags. This ensures that the session ID will not be accessible to client-side scripts and it will only be transmitted over HTTPS.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.5.4

20.10.2 10.2 Maturity Level 2

10.2.1 Requirement: Regenerate session tokens

Details: Regenerate session tokens when the user authenticates to the application. Additionally, should the encryption status change, the session token must be regenerated.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.5.10
- NIST 800-53r5 SC-23(3)

10.2.2 Requirement: Ensure that session identifiers are sufficiently random

Details: Session tokens must be generated by secure random functions and must be at least 128 bits or provide 64 bits of entropy.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.5.5
- NIST 800-53r5 SC-23(3)

10.2.3 Requirement: Invalidate the session after logout

Details: When the user logs out of the application, the session on the server must be destroyed. This ensures that the session cannot be accidentally revived.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.5.6
- CIS Controls v8 4.3
- NIST 800-53r5 AC-12

20.10.3 10.3 Maturity Level 3

10.3.1 Requirement: Destroy sessions at any sign of tampering

Details: Unless the application requires multiple simultaneous sessions for a single user, implement features to detect session cloning attempts. Should any sign of session cloning be detected, the session must be destroyed, forcing the real user to reauthenticate.

Applies to: Web components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.5.7

10.3.2. Requirement: Lock endpoint device sessions after inactivity

Details: Product must provide capability to automatically lock endpoint device sessions after a standard period of inactivity. This is a basic security control that should be used universally. Employees should also be trained to lock their computers whenever they leave them.

Applies to: On-premises components

References

- CIS Security Best Practices for Non-Voting Election Technology 5.1.11
- CIS Controls v8 4.3
- NIST 800-53r5 AC-2(5), AC-11, AC-11(1), AC-12

10.3.3 Requirement: Implement an idle session timeout

Details: When a user is not active for a period of time, the application should automatically log the user out.

> Be aware that Ajax applications may make recurring calls to the application, effectively resetting the timeout counter automatically.

Applies to: All components

References

- CIS Security Best Practices for Non-Voting Election Technology A1.5.9
- CIS Controls v8 4.3
- NIST 800-53r5 AC-12

INDEX

A

Accredited Assessor Organization, 69
Activity, 69
Architecture Assessment, 69
Architecture Maturity Score, 69

B

BPMN, 69
Business Process Model and Notation, 69

C

Component, 69
Composite Service, 69
Conditional, 50

D

Draft, 50

F

Final, 50
Function, 69

I

In-scope Services, 70
Initial Product Submission, 70
Isolation, 70

M

Modularity, 70

N

Not Verified, 50

O

Organizational Assessment, 70
Organizational Maturity Score, 70

P

Port, 70
Product, 70
Product Implementation Score, 70
Product Revision, 70
Product Revision Submission, 70
Product Submission, 70
Product Verification, 70

R

RABET-V Administrator, 71
RABET-V Iteration, 71
RABET-V Portal, 71
RABET-V Public Listing Site, 71
RABET-V Strategic Advisory Committee, 71
Registered Technology Provider, 71
Reliability, 71
Required Security Services, 71
RTP, 71

S

Security Control Family, 71
Security Enclave, 71
Security Service, 71
Security Services Architecture, 71
Services, 71

T

Test Plan, 72
Transparent Service, 72

V

Verified, 51