FR-COMP-005 — DISA STIG Compliance Baselines

Go to Crucible Compliance Management Requirements

Statement

Crucible SHALL provide Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) Compliance Baselines.

Derived From

This requirement derives from:

- Crucible System Requirements Specification, Version 1.1 Draft, Functional Requirements, FR-COMP-005

The Original Requirement states:

> *The system shall support DISA STIG compliance baselines.*[C1]

FR-COMP-005:

- Replaces **The system** with the defined system name Crucible
- Changes **shall** to the established uppercase normative form **SHALL**
- Replaces the weak verb **support** with **provide**
- Links **DISA**, **STIG**, and **Compliance Baselines** to their controlling definitions
- Preserves DISA STIG as the source-identified compliance framework

No other substantive normalization is required.

Rationale

The Defense Information Systems Agency (DISA) publishes Security Technical Implementation Guides (STIGs) that provide security configuration guidance and associated evaluation criteria for specified technologies.

A DISA STIG Compliance Baseline enables Crucible compliance activities to use criteria derived from an identified STIG.

Such a Compliance Baseline can include:

- Security configuration requirements

- Evaluation criteria
- Expected values
- Severity classifications
- Applicability conditions
- Check procedures
- Remediation guidance
- References to the source STIG
- References to related security controls

This requirement establishes provision of DISA STIG Compliance Baselines without prescribing:

- Which STIGs Crucible provides
- A particular STIG revision
- The process used to create or import a Compliance Baseline
- Application of a Compliance Baseline
- Compliance scanning
- Compliance assessment
- Remediation
- Compliance reporting
- Evidence generation
- Automatic updates
- Approval or lifecycle management

Separate requirements, architecture specifications, workflows, or policies define those subjects and behaviors.

Applies To

This requirement applies to:

- Crucible
- Defense Information Systems Agency (DISA)
- Security Technical Implementation Guides (STIGs)
- DISA STIG Compliance Baselines

Verification

Verification confirms that:

1. A Security Technical Implementation Guide (STIG) is selected for testing
2. Crucible provides a Compliance Baseline associated with the selected STIG
3. The provided Compliance Baseline identifies the DISA STIG from which it derives
4. The compliance criteria represented by the provided Compliance Baseline can be determined
5. The resulting Compliance Baseline can be identified

Referenced By

The following pages reference this requirement:

- 5.4 Assess Compliance
- 6.1 Construct and Assess the Environment
- 8.1 Select Compliance Criteria and Baselines
- Annex D: Requirements Traceability

Implementation Status

Implemented and Verified

Requirement Status

☐ Review and approve FR-COMP-005 as a leaf requirement.

Issues

☐ Determine whether separate requirements identify the DISA STIG products and revisions that Crucible must provide.

☐ Determine whether separate requirements govern importing, updating, approving, and applying DISA STIG Compliance Baselines.

Notes for Editors

This requirement page retains the stable requirement identifier `FR-COMP-005`.

This page is a leaf requirement page and omits a trailing `:start` from its namespace.

The Statement preserves the approved source intent by requiring Crucible to provide DISA STIG Compliance Baselines.

Use the following controlling Terms and Definitions entries:

- Defense Information Systems Agency (DISA)
- Security Technical Implementation Guide (STIG)
- Compliance Baseline

Do not change **provide** to **define**, **import**, **maintain**, **apply**, **scan against**, or **assess against** unless the controlling requirement identifies that specific behavior.

Do not add a particular STIG, STIG revision, operating system, scanning tool, update mechanism, remediation process, reporting obligation, or Evidence-generation obligation unless the controlling requirement changes through an approved requirements process.

To reference this requirement Statement from another wiki page, insert:

```
{{section>dido:02-crusible:99-annexes:annex-c-requirements:03-functional-requirements:03-06-compliance-management:fr-comp-005#Statement&noheader&nofooter&noeditbtn}}
```
