8.1 Select Compliance Criteria and Baselines

Go to 8. Compliance Operations

Before performing a Compliance Assessment, the applicable organization identifies the compliance criteria and Compliance Baseline against which Crucible evaluates the assessment subject.

Crucible supports defined Compliance Baselines, including:

- DISA STIG Compliance Baselines
- FedRAMP Baseline Definitions
- Custom Compliance Frameworks
- Other Compliance Baselines represented through the supported baseline-definition capability

The selection establishes the criteria for the assessment. It does not independently determine which legal, regulatory, contractual, security, or organizational obligations apply to the subject.

Identify the Assessment Subject

The compliance operation identifies the subject to which the selected criteria apply.

An assessment subject can include:

- A Machine Image
- A Container Image
- An Infrastructure Configuration
- An Infrastructure Environment
- A deployed resource
- Another identified artifact supported by the applicable Compliance Baseline

The subject remains identifiable by the information needed to distinguish it from another artifact, resource, environment, or revision.

Identify the Applicable Compliance Obligations

The responsible organization determines the compliance obligations applicable to the assessment subject.

Those obligations can derive from:

- Organizational security policy
- A government security program
- A regulatory obligation
- A contractual obligation
- A deployment-environment requirement
- A Security Domain policy
- An approved custom compliance framework

Crucible does not independently decide which obligation governs the subject.

Select a Compliance Baseline

The compliance operation selects a Compliance Baseline that represents the criteria applicable to the identified subject.

The selected Compliance Baseline identifies:

- The Baseline
- The Baseline revision
- The Baseline source
- The included compliance criteria
- The subject or subject type to which the Baseline applies
- Applicable profiles, parameters, or tailoring information
- The compliance framework represented by the Baseline

The assessment uses the identified Baseline revision rather than an unspecified or changing set of criteria.

DISA STIG Compliance Baselines

Crucible supports Compliance Baselines based on Defense Information Systems Agency Security Technical Implementation Guides.

A selected DISA STIG Compliance Baseline identifies the STIG content and revision applicable to the assessment subject.

Support for a DISA STIG Compliance Baseline does not establish that:

- Every STIG applies to the subject
- Every STIG criterion can be evaluated by the selected assessment tool
- The subject satisfies the selected STIG
- An exception or deviation has been approved
- The subject has received operational authorization

The applicable organization determines the selected STIG, tailoring, exceptions, and acceptance process.

FedRAMP Baseline Definitions

Crucible supports definitions representing applicable FedRAMP Baselines.

The selected definition identifies the FedRAMP Baseline and revision used to organize or relate the applicable compliance criteria.

Support for a FedRAMP Baseline Definition does not grant FedRAMP authorization or establish that the complete system satisfies FedRAMP requirements.

Custom Compliance Frameworks

Crucible supports organization-defined or otherwise approved custom compliance frameworks.

A custom compliance framework can represent criteria not completely addressed by a predefined Compliance Baseline.

The custom framework identifies:

- The framework
- The framework revision
- The governing source or organization
- The included compliance criteria
- The subjects to which the framework applies
- Applicable parameters or tailoring information

A custom framework remains a controlled compliance definition rather than an undocumented collection of assessment checks.

Select the Applicable Criteria

The selected Compliance Baseline can contain more criteria than apply to a particular subject or assessment activity.

The responsible organization identifies the applicable criteria and any approved:

- Profiles
- Parameters
- Tailoring decisions
- Exceptions
- Exclusions
- Alternative criteria

Crucible preserves the selected baseline and criteria as inputs to the subsequent Compliance Assessment.

An exclusion from the selected assessment does not by itself establish an approved compliance exception or risk acceptance.

Selection Result

The selection result identifies:

- The assessment subject

- The selected Compliance Baseline
- The Baseline revision
- The represented compliance framework
- The applicable compliance criteria
- Applicable parameters or tailoring information
- The source of the selected Baseline
- Any approved exception or exclusion reference provided as an assessment input

The selected criteria and Compliance Baseline become controlled inputs to 8.2 Perform Compliance Assessments.

Requirements Addressed

Requirement	Statement
FR-COMP-001 — Compliance Baseline Definitions	Crucible SHALL define Compliance Baselines.
FR-COMP-005 — DISA STIG Compliance Baselines	Crucible SHALL provide Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) Compliance Baselines.
FR-COMP-006 — FedRAMP Baseline Definitions	Crucible SHALL define Federal Risk and Authorization Management Program (FedRAMP) Compliance Baselines.
FR-COMP-007 — Custom Compliance Frameworks	Crucible SHALL define user-defined Compliance Frameworks.

The linked leaf requirement pages remain the canonical sources.
