5.4 Assess Compliance

Go to 5. Operational Concept

Crucible performs a Compliance Assessment by evaluating an identified subject against selected compliance criteria.

The assessed subject can include:

- A Machine Image
- A Container Image
- An Infrastructure Environment
- An Infrastructure Configuration
- A deployed resource or workload
- A Baseline
- Another identified artifact or operational result governed by applicable compliance criteria

The assessment identifies the subject, applicable criteria, assessment provider, observed results, Compliance Findings, and supporting Evidence.

Select Compliance Criteria

Crucible selects or receives the compliance criteria applicable to the assessed subject.

The criteria can derive from:

- A Compliance Baseline
- A Compliance Benchmark
- An organizational policy
- A regulatory or contractual obligation
- An approved security framework
- A user-defined compliance framework
- Criteria associated with a selected Deployment Target or Security Domain

The selected criteria identify the conditions used to evaluate the subject. Crucible does not independently determine which legal, regulatory, contractual, or organizational obligations apply.

Compliance Baselines

A Compliance Baseline defines a controlled set of compliance criteria applicable to one or more assessment subjects.

Crucible preserves:

- The Compliance Baseline identifier
- The selected revision
- The source or governing authority

- The subject types to which the Baseline applies
- The included criteria
- Applicable parameters or profiles
- The relationship between the Baseline and the assessed subject

Crucible can use established or organization-defined Compliance Baselines, including Baselines derived from DISA STIGs, FedRAMP, or other approved frameworks.

Support for a named framework does not cause Crucible to grant certification, authorization, or approval under that framework.

Assessment Providers

Crucible can integrate with one or more compliance-scanning or assessment tools through controlled provider interfaces.

An assessment provider performs provider-specific evaluation behavior while Crucible preserves the provider-independent assessment intent and lifecycle records.

The provider integration identifies:

- The assessment provider
- The provider implementation and revision
- The assessed subject
- The selected compliance criteria
- Provider-specific parameters
- The assessment invocation
- The results returned by the provider

The assessment abstraction is not limited to one operating system, assessment product, or provider implementation.

Different assessment providers can produce different native result formats. Crucible preserves sufficient information to relate each provider result to the assessed subject, selected criteria, and resulting Compliance Findings.

Perform the Compliance Assessment

Crucible evaluates the identified subject against the selected compliance criteria using the applicable assessment provider.

The assessment process can include:

1. Identify the assessment subject
2. Select the applicable Compliance Baseline or criteria
3. Select an approved assessment provider
4. Supply the required provider parameters
5. Execute the assessment

6. Receive and preserve the provider results
7. Normalize or relate the results to the applicable criteria
8. Produce Compliance Findings
9. Generate the applicable report and supporting Evidence

A Compliance Assessment evaluates the subject as it exists at the time of assessment. A later change to the subject, criteria, provider, or configuration can require another assessment.

Compliance Findings

A Compliance Finding records the result of evaluating an identified subject against an identified compliance criterion.

A finding can identify:

- The assessed subject
- The applicable criterion
- The observed condition
- The assessment result
- The assessment provider
- The assessment time
- The applicable severity or classification
- Supporting Evidence
- An exception, waiver, or remediation reference, when applicable

A finding reports the observed relationship between the subject and the criterion. The responsible authority determines whether the finding requires remediation, exception approval, risk acceptance, or another action.

Compliance Reports

Crucible produces a compliance report that presents the results of an identified Compliance Assessment.

The report can contain:

- The assessed subject and revision
- The selected Compliance Baseline or criteria
- The assessment provider and revision
- The assessment time
- The assessment status
- The applicable Compliance Findings
- Summary counts or classifications
- Exceptions or unresolved conditions
- References to supporting Evidence
- Provenance and Traceability information

The report does not replace the underlying findings, provider results, or Evidence.

Supporting Evidence

Crucible generates and preserves Evidence associated with the Compliance Assessment.

The Evidence can support:

- Review of individual Compliance Findings
- Confirmation of the subject and criteria assessed
- Reproduction or reevaluation of the assessment
- Security-control implementation review
- Security Controls Traceability Matrix activities
- Risk Management Framework activities
- Authority to Operate processes
- Audit and governance activities

Crucible provides supporting Evidence but does not grant Accreditation, Operational Approval, or an Authority to Operate (ATO).

Connected and Disconnected Assessment

A Compliance Assessment can occur in a Connected Environment, Disconnected Environment, or Air-Gapped Environment when the required criteria, assessment provider, dependencies, and supporting resources are available within the applicable boundary.

Compliance Findings produced during connected operation can accompany the artifacts they describe into a disconnected environment.

Crucible preserves the relationship among:

- The assessed artifact
- The applicable Compliance Baseline
- The assessment provider
- The Compliance Findings
- The supporting Evidence
- The applicable Transfer Bundle
- The source and destination environments

The transfer process does not change the meaning or status of a Compliance Finding. A subsequent change to the transferred artifact or its environment can require reassessment.

Assessment Result

The Compliance Assessment result records:

- The assessment identifier
- The assessed subject and revision

- The selected Compliance Baseline or criteria
- The assessment provider and revision
- The provider-specific parameters
- The assessment time
- The provider results
- The Compliance Findings
- The compliance report
- The supporting Evidence
- The associated Provenance
- The associated Traceability
- The transfer relationship, when applicable

The assessment result becomes an input to remediation, image promotion, deployment validation, transfer, authorization-supporting activities, or subsequent reassessment.

Requirements Addressed

Requirement	Statement
FR-COMP-001 — Compliance Baseline Definitions	Crucible SHALL define Compliance Baselines.
FR-COMP-002 — Compliance Scanning Tool Integration	Crucible SHALL integrate with Compliance Scanning Tools.
FR-COMP-003 — Compliance Reporting	Crucible SHALL generate Compliance Reports.
FR-COMP-004 — Compliance Evidence Artifacts	Crucible SHALL generate Compliance Evidence Artifacts.
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	
fr-comp-007	
FR-COMP-008a — Compliance Scanning Abstraction	Crucible SHALL provide a Compliance Scanning Abstraction.
FR-COMP-008b — Multiple Operating-System Support	Crucible SHALL evaluate two or more Operating Systems against defined compliance criteria.
FR-COMP-009a — Security Control Traceability Matrix Evidence	Crucible SHALL generate Security-Control Implementation Evidence for inclusion in a Security Control Traceability Matrix (SCTM).
FR-COMP-009b — Risk Management Framework Evidence	Crucible SHALL generate Security-Control Implementation Evidence for use in Risk Management Framework (RMF) activities.
FR-COMP-009c — Authorization to Operate Evidence	Crucible SHALL generate Security-Control Implementation Evidence for use in Authorization to Operate (ATO) activities.
FR-COMP-010a — Compliance Finding Transfer Bundle Inclusion	Crucible SHALL include Compliance Findings in the Transfer Bundle containing the Artifacts to which the Compliance Findings apply.

Requirement	Statement
FR-COMP-010b — Compliance Finding Association Preservation	Crucible SHALL preserve the association between each Compliance Finding and the Artifact to which the Compliance Finding applies when transferring them in a Transfer Bundle from a Connected Environment to a Disconnected Environment.

The linked leaf requirement pages remain the canonical sources.
