6.1 Construct and Assess the Environment

Go to 6. Connected Operations

Within a Connected Environment, Crucible constructs controlled Images and assesses identified subjects against applicable compliance criteria.

Connectivity provides access to the authorized resources required by the applicable construction and assessment activities. The Image Management and Compliance Management requirements define the capabilities performed. Connected operation does not establish a separate source-access capability.

Prepare the Controlled Inputs

Crucible uses the applicable controlled inputs for the selected construction or assessment activity.

Construction inputs can include:

- A selected Baseline Composition
- A base Machine Image or Container Image
- Selected Image Layers
- Application content
- Software packages
- Configuration definitions
- Security configuration
- Build dependencies
- Applicable build parameters

Assessment inputs can include:

- The identified assessment subject
- The applicable Compliance Baseline
- Compliance criteria
- Assessment content
- The selected assessment provider
- Provider-specific parameters

The applicable lifecycle definition identifies the inputs required for each activity.

Construct the Image

Crucible constructs an identified Machine Image or Container Image from the selected controlled inputs.

The construction activity can include:

1. Select the applicable image form
2. Select the controlled build inputs

3. Execute the applicable construction process
4. Produce the resulting Image
5. Assign the Image identifier and revision
6. Record the Image content digest
7. Sign the Image when required
8. Verify the Image signature when required
9. Apply the applicable promotion transition

When a required change affects a deployed immutable Image, Crucible constructs a replacement Image rather than modifying the deployed Image in place.

Image construction does not independently establish compliance or authorization for deployment.

Select the Compliance Criteria

Crucible identifies the compliance criteria applicable to the assessment subject.

The criteria can derive from:

- A Compliance Baseline
- A DISA STIG Compliance Baseline
- A FedRAMP Baseline
- A custom compliance framework
- Another approved set of compliance criteria

The responsible organization determines which compliance criteria apply to the assessment subject.

Perform the Compliance Assessment

Crucible integrates with an applicable compliance-scanning or assessment tool and evaluates the identified subject against the selected compliance criteria.

The assessment activity can include:

1. Identify the assessment subject
2. Select the applicable Compliance Baseline or criteria
3. Select the assessment provider
4. Supply the required assessment parameters
5. Execute the assessment
6. Receive the assessment results
7. Produce the applicable Compliance Findings
8. Generate the compliance report
9. Generate the Compliance Evidence Artifacts

The compliance-scanning abstraction separates the assessment activity from a particular operating system or scanning product.

Support for multiple operating systems does not require every assessment provider to support every

operating system.

Review the Assessment Results

The assessment result identifies the relationship between the assessed subject and the applicable compliance criteria.

The result can include:

- The assessed subject and revision
- The selected Compliance Baseline or criteria
- The assessment provider
- The assessment results
- Compliance Findings
- The compliance report
- Compliance Evidence Artifacts
- Security-control implementation Evidence
- Transferable Compliance Findings, when applicable

Crucible generates Evidence that can support Security Control Traceability Matrix, Risk Management Framework, and Authority to Operate activities.

Crucible does not grant Accreditation, Operational Approval, risk acceptance, or an Authority to Operate.

Connected-Operation Result

The connected construction and assessment activities produce identifiable results that can include:

- A constructed Machine Image or Container Image
- An Image identifier and revision
- An Image content digest
- A Digital Signature
- A signature-verification result
- An Image promotion result
- Compliance Findings
- A compliance report
- Compliance Evidence Artifacts
- Security-control implementation Evidence
- Transferable Compliance Findings

The applicable lifecycle activity determines which results Crucible produces.

Requirements Addressed

Requirement	Statement
FR-IMG-001 — Build Virtual Machine Images	Crucible SHALL build Machine Images.
FR-IMG-002 — Build Container Images	Crucible SHALL build Container Images.
FR-IMG-003 — Immutable Infrastructure Workflows	Crucible SHALL apply changes to deployed images by replacing the images rather than modifying them in place.
FR-IMG-004 — Image Signing	Crucible SHALL generate a Digital Signature for an identified Image and associate the Digital Signature with that Image.
FR-IMG-005 — Image Verification	Crucible SHALL verify the Digital Signature associated with an identified Image.
FR-IMG-006 — Image Promotion Workflows	Crucible SHALL perform Image Promotion for an identified Image after the Image satisfies the applicable transition criteria.
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 — 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.
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.
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.