OR-003 — Classified and Unclassified Environments

Go to Operational Requirements

Original Requirement

> *The system SHALL support classified and unclassified deployment environments.*[C1]

Assessment of Original Requirement

The Original Requirement preserves the approved operational intent but does not express independently testable normative statements.

The following Specification Discipline and Authoring findings apply:

- **The system** does not use the defined system name Crucible
- **Support** is a weak verb that does not identify an observable behavior performed by Crucible
- **Classified and unclassified** combines two operating contexts that can pass or fail independently
- **Deployment environments** does not identify the Operational Lifecycle activities that Crucible performs
- The Original Requirement does not identify the Security Domain governing an environment
- The Original Requirement does not identify the Security Classification authorized for a Classified Environment
- The Original Requirement does not identify the Classification Authority governing classified information
- The Original Requirement does not require enforcement of access restrictions
- The Original Requirement does not require enforcement of Information Handling Rules
- The Original Requirement does not identify the conditions governing movement of information between Security Domains
- The Original Requirement does not require use of an authorized Cross-Domain Transfer
- The Original Requirement does not identify the behavior required when information is not authorized for an operation or destination
- The Original Requirement does not provide independently identifiable statements for verification and Traceability

The previously normalized Statement also combined:

- Execution of selected Operational Lifecycle activities within Classified Environments
- Execution of selected Operational Lifecycle activities within Unclassified Environments
- Restriction of operations to the governing Security Domain
- Enforcement of access restrictions
- Enforcement of Information Handling Rules
- Control of information transfer between Security Domains

These obligations can pass or fail independently.

For example:

- Crucible can operate successfully in an Unclassified Environment and fail in a Classified Environment
- Crucible can enforce access restrictions and fail to enforce Information Handling Rules
- Crucible can operate within both environment types and permit an unauthorized Cross-Domain Transfer
- Crucible can enforce Security Domain boundaries for users while failing to restrict an automated process
- Crucible can reject an unauthorized transfer while failing to preserve the required transfer record

The Original Requirement therefore requires decomposition into independently identifiable normative requirements.

The decomposition preserves `OR-003` as the stable parent requirement identifier. Each proposed replacement requirement receives a lettered identifier and a separate leaf requirement page.

Proposed Statements

The Original Requirement is decomposed into the following proposed replacement requirements:

- OR-003a — Classified Environment Operations
- OR-003b — Unclassified Environment Operations
- OR-003c — Security Domain Enforcement
- OR-003d — Information Handling Rule Enforcement
- OR-003e — Cross-Domain Transfer Control
- OR-003f — Security Domain Access Control

- OR-003a — Classified Environment Operations
- OR-003b — Unclassified Environment Operations
- OR-003c — Security Domain Resource Enforcement
- OR-003d — Security Domain Information Enforcement
- OR-003e — Information Handling Rule Enforcement
- OR-003f — Cross-Domain Transfer Control
- OR-003g — Security Domain Access Control

Requirement Status

☐ Review and approve the proposed decomposition of OR-003 into independently testable Classified Environment operations, Unclassified Environment operations, Security Domain enforcement, Information Handling Rule enforcement, Cross-Domain Transfer control, and Security Domain access-control requirements.

☐ Determine whether OR-003a through OR-003f collectively preserve the complete approved intent

of OR-003.

☐ Determine whether OR-003a through OR-003f collectively supersede OR-003.

☐ If the proposed child requirements are accepted as the complete replacement for OR-003, mark OR-003 as superseded and preserve this page as the parent Traceability record.

Issues

The following unresolved issues affect the decomposition of OR-003:

☐ Define the Operational Lifecycle activities that Crucible must execute within Classified Environments.

☐ Define the Operational Lifecycle activities that Crucible must execute within Unclassified Environments.

☐ Identify the Security Classifications that each supported Classified Environment is authorized to handle.

☐ Identify the Classification Authority governing each Security Classification used by Crucible.

☐ Define the Security Domain boundaries governing each Classified Environment and Unclassified Environment.

☐ Define the resources, information, operations, users, and processes authorized within each Security Domain.

☐ Define the Information Handling Rules governing each Security Classification and handling designation.

☐ Define how Crucible associates Information Handling Rules with information and information-bearing Artifacts.

☐ Define the behavior required when information lacks a Security Classification or handling designation.

☐ Define the Cross-Domain Transfer mechanisms authorized between supported Security Domains.

☐ Define the authorization required for each Cross-Domain Transfer.

☐ Define the validation, integrity, inspection, and destination-acceptance requirements for Cross-Domain Transfers.

☐ Define the behavior required when information is not authorized for the destination Security Domain.

☐ Define the identity, role, authorization, and need-to-know information used to control access within a Security Domain.

☐ Define the behavior required when an automated process lacks authorization for a requested operation, resource, or information object.

☐ Determine whether OR-003a through OR-003f provide complete coverage of the approved intent of OR-003.

Notes for Editors

This page should retain the stable parent requirement identifier `OR-003`.

This page is a non-leaf requirement page and retains a trailing `:start` in its namespace.

The child requirements are leaf requirement pages and omit a trailing `:start` from their namespaces.

The explicit child-page links should remain while the proposed decomposition is being developed. After the child pages have been created and finalized, the explicit links may be removed because the `indexmenu` displays the child requirement pages contained within the OR-003 namespace.

This page preserves:

- The Original Requirement
- The assessment of the Original Requirement
- The reason for decomposition
- Traceability to the proposed replacement requirements
- The unresolved cross-cutting issues affecting the decomposition
- The supersession decision

The derived requirements should distinguish:

- Execution of Operational Lifecycle activities within Classified Environments
- Execution of Operational Lifecycle activities within Unclassified Environments
- Restriction of operations, resources, and information to the governing Security Domain
- Enforcement of Information Handling Rules
- Control of information movement through authorized Cross-Domain Transfers
- Restriction of access according to identity, role, authorization, need to know, and Security Domain

The proposed child Statements should retain the following intent:

- OR-003a requires Crucible to execute selected Operational Lifecycle activities within a Classified Environment
- OR-003b requires Crucible to execute selected Operational Lifecycle activities within an Unclassified Environment
- OR-003c requires Crucible to restrict each operation to resources and information authorized for the governing Security Domain
- OR-003d requires Crucible to enforce the Information Handling Rules governing each information object processed by a Crucible operation
- OR-003e requires Crucible to transfer information between Security Domains only through an

authorized Cross-Domain Transfer
- OR-003f requires Crucible to permit a user or process to access only operations, resources, and information authorized for its identity, role, and Security Domain

The Original Requirement should not be marked as superseded until the requirement owner:

- Approves the proposed decomposition
- Approves the child requirements
- Defines the Operational Lifecycle activities required in each environment type
- Defines the supported Security Domains
- Defines the governing Security Classifications and Classification Authorities
- Defines the Information Handling Rules
- Defines the authorized Cross-Domain Transfer mechanisms
- Defines the access-control model
- Confirms that the child requirements collectively preserve the complete approved intent of OR-003
- Confirms that no additional child requirements are required

After supersession, this page should remain as the parent Traceability record and should continue to preserve the Original Requirement and its assessment.

Material changes to the decomposition should update the child requirements, Requirement Status, Issues, and Traceability records.
