OR-003c — Security Domain Enforcement

Go to OR-003 — Classified and Unclassified Environments

Statement

Crucible SHALL restrict each operation to the resources and information authorized for its governing Security Domain.

Derived From

This requirement derives from:

- OR-003 — Classified and Unclassified Environments
- Crucible System Requirements Specification, Version 1.1 Draft, Operational Requirements, OR-003

The Original Requirement states:

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

OR-003c isolates the obligation to enforce the resource and information boundaries established for the Security Domain governing a Crucible operation.

Rationale

A Classified Environment or Unclassified Environment can contain multiple Security Domains governed by different security policies, authorities, missions, compartments, or release restrictions.

Successful operation within an environment does not by itself demonstrate that an operation remained within its authorized Security Domain.

OR-003c requires Crucible to enforce the resource and information boundaries of the Security Domain governing each operation.

The responsible authority establishes the Security Domain, its boundary, and its authorizations. Crucible enforces those established authorizations and does not create the Security Domain through execution of this requirement.

Applies To

This requirement applies to:

- Crucible
- Security Domains
- Crucible operations
- Information processed by Crucible operations
- Resources accessed by Crucible operations
- Classified Environments
- Unclassified Environments

Verification

Verification confirms that:

1. Each tested Crucible operation identifies its governing Security Domain
2. The governing Security Domain identifies the resources authorized for the tested operation
3. The governing Security Domain identifies the information authorized for the tested operation
4. Crucible permits the tested operation to access resources authorized for the governing Security Domain
5. Crucible permits the tested operation to process information authorized for the governing Security Domain
6. Crucible denies the tested operation access to resources not authorized for the governing Security Domain
7. Crucible denies the tested operation access to information not authorized for the governing Security Domain
8. Crucible records each denial caused by a Security Domain restriction
9. Each denial record identifies the operation, governing Security Domain, requested resource or information, and denial result

Referenced By

The following pages reference this requirement:

- 3.3 Security Domains and Transfer Boundaries
- 4.1 Human Actors
- 4.3 External Systems
- Annex D: Requirements Traceability

Delivery Phase

☐ Determine the Delivery Phase for OR-003c.

Implementation Status

☐ Assess whether the current Crucible implementation restricts each operation to the resources and

information authorized for its governing Security Domain.

Requirement Status

☐ Review and approve OR-003c as a leaf requirement derived from OR-003.

Issues

☐ Identify the authority responsible for establishing each Security Domain used by Crucible.

☐ Define how each Crucible operation identifies its governing Security Domain.

☐ Define how each Security Domain identifies its authorized resources.

☐ Define how each Security Domain identifies its authorized information.

☐ Define the behavior required when an operation does not identify a governing Security Domain.

☐ Define the behavior required when a requested resource or information object lacks a Security Domain association.

☐ Define the record required when Crucible denies an operation because of a Security Domain restriction.

Notes for Editors

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

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

OR-003c requires enforcement of an established Security Domain. It does not require Crucible to establish, authorize, or define a Security Domain.

The responsible authority establishes:

- The Security Domain identifier
- The Security Domain boundary
- The governing security policy
- The authorized resources
- The authorized information
- The entities permitted to operate within the Security Domain

Changes to the Statement should preserve:

- Crucible as the responsible actor

- Restriction as the required behavior
- Each Crucible operation as the subject of enforcement
- The governing Security Domain as the source of authorization
- Resources and information as the objects governed by the restriction

Requirements governing user or process authorization should remain in OR-003f — Security Domain Access Control.

Requirements governing the handling of authorized information should remain in OR-003d — Information Handling Rule Enforcement.

Requirements governing movement between Security Domains should remain in OR-003e — Cross-Domain Transfer Control.

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

```
{{section>dido:02-crusible:99-annexes:annex-c-requirements:02-operational-requirements:or-003:or-003c#Statement&noheader&nofooter&noeditbtn}}
```

Do not rename this page after an external citation unless a redirect or move plan is in place.
