OR-003g — Security Domain Access Control

Go to OR-003 — Classified and Unclassified Environments

Statement

Crucible SHALL deny an access request that the governing Security Domain does not authorize for the requesting identity.

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-003g isolates the obligation to deny access requests not authorized for the requesting identity within the governing Security Domain.

Rationale

Operation within an authorized Classified Environment or Unclassified Environment does not authorize every identity to access every operation, resource, or information object within that environment.

A Security Domain establishes the authorization boundary governing identities and access requests within its scope.

OR-003g requires Crucible to deny an access request when the governing Security Domain does not authorize the requesting identity to perform the requested access.

Applies To

This requirement applies to:

- Crucible
- Security Domains
- Requesting identities

- Access requests
- Crucible operations
- Resources accessed through Crucible
- Information accessed through Crucible
- Classified Environments
- Unclassified Environments

Verification

Verification confirms that:

1. Each tested access request identifies the requesting identity
2. Each tested access request identifies its governing Security Domain
3. Each tested access request identifies the requested access
4. The governing Security Domain provides an authorization decision for the requesting identity and requested access
5. Crucible permits an access request authorized for the requesting identity
6. Crucible denies an access request not authorized for the requesting identity
7. Crucible denies an access request when the requesting identity cannot be determined
8. Crucible denies an access request when the governing Security Domain cannot be determined
9. Crucible records each access denial
10. Each denial record identifies the requesting identity, governing Security Domain, requested access, 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-003g.

Implementation Status

☐ Assess whether the current Crucible implementation denies access requests not authorized for the requesting identity within the governing Security Domain.

Requirement Status

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

Issues

☐ Define how Crucible identifies and authenticates the identity making an access request.

☐ Define how each access request identifies its governing Security Domain.

☐ Define how the governing Security Domain represents authorization for an identity and requested access.

☐ Define the access actions subject to authorization.

☐ Define the behavior required when the requesting identity cannot be authenticated.

☐ Define the behavior required when the governing Security Domain cannot be determined.

☐ Define the behavior required when an authorization decision cannot be obtained.

☐ Define the record required when Crucible denies an access request.

Notes for Editors

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

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

OR-003g governs whether a requesting identity may perform requested access within a Security Domain.

The responsible authority establishes:

- The recognized identity types
- The authentication requirements
- The roles or attributes associated with an identity
- The access actions subject to authorization
- The authorization policy
- The conditions under which access is permitted or denied

Changes to the Statement should preserve:

- Crucible as the responsible actor
- Denial as the required behavior

- An access request as the evaluated subject
- The requesting identity as the entity seeking access
- The governing Security Domain as the source of authorization

OR-003g differs from the other Security Domain requirements:

- OR-003c prevents an operation from accessing an unauthorized resource
- OR-003d prevents an operation from processing unauthorized information
- OR-003e enforces the Information Handling Rules governing authorized information
- OR-003f controls information transfer between Security Domains
- OR-003g determines whether the requesting identity is authorized to perform the requested access

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-003g#Statement&noheader&nofooter&noeditbtn}}
```

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