FR-COMP-009a — Security Control Traceability Matrix Evidence

Go to FR-COMP-009 — Security-Control Implementation Evidence

Statement

Crucible SHALL generate Security-Control Implementation Evidence for inclusion in a Security Control Traceability Matrix (SCTM).

Derived From

This requirement derives from:

- FR-COMP-009 — Security-Control Implementation Evidence
- Crucible System Requirements Specification, Version 1.1 Draft, Functional Requirements, FR-COMP-009

The Original Requirement states:

> *The system shall generate security-control implementation evidence suitable for supporting SCTM, RMF, and ATO processes.*[C1]

FR-COMP-009a:

- Replaces **The system** with the defined system name Crucible
- Changes **shall** to the established uppercase normative form **SHALL**
- Extracts generation of Security-Control Implementation Evidence for the SCTM context as an independently verifiable requirement
- Replaces the weak phrase **suitable for supporting SCTM processes** with the direct purpose **for inclusion in a Security Control Traceability Matrix**
- Assigns RMF Evidence to FR-COMP-009b
- Assigns ATO Evidence to FR-COMP-009c

Rationale

A Security Control Traceability Matrix (SCTM) records traceable relationships between Security Controls and associated implementation, assessment, finding, remediation, and Evidence information.

Security-Control Implementation Evidence generated for inclusion in an SCTM enables a reviewer to associate the Evidence with the Security Control implementation that the Evidence describes.

This requirement establishes generation of Security-Control Implementation Evidence for inclusion in

an SCTM without requiring Crucible to:

- Create or maintain the complete SCTM
- Approve a Security Control implementation
- Determine whether a Security Control operates effectively
- Perform the responsibilities of a control assessor
- Resolve Compliance Findings
- Make a risk-management decision
- Issue an Authorization to Operate (ATO)

Separate requirements, architecture specifications, evidence profiles, or procedures govern those subjects and behaviors.

Applies To

This requirement applies to:

- Crucible
- Security-Control implementations
- Security-Control Implementation Evidence
- Security Control Traceability Matrices (SCTMs)

Verification

Verification confirms that:

1. A Security Control implementation is selected for testing
2. Crucible generates Security-Control Implementation Evidence for the selected implementation
3. The generated Evidence can be associated with the Security Control represented in a Security Control Traceability Matrix (SCTM)
4. The generated Evidence can be included in the SCTM
5. The association between the SCTM entry and the generated Evidence can be determined

Referenced By

The following pages reference this requirement:

- 5.4 Assess Compliance
- 5.7 Preserve Evidence and Lifecycle Records
- 6.1 Construct and Assess the Environment
- 8.4 Generate Supporting Evidence
- Annex D: Requirements Traceability

Implementation Status

Implemented and Verified

Requirement Status

☐ Review and approve FR-COMP-009a as a leaf requirement.

Issues

☐ Determine whether Security Control requires a controlled definition in the shared Terms and Definitions corpus.

☐ Determine whether Security-Control Implementation Evidence requires a controlled definition in the shared Terms and Definitions corpus.

☐ Determine whether a separate requirement defines the minimum identifiers and references required to associate the Evidence with an SCTM entry.

Notes for Editors

This requirement page retains the derived requirement identifier `FR-COMP-009a`.

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

The namespace for this requirement is:

`dido:02-crusible:99-annexes:annex-c-requirements:03-functional-requirements:03-06-compliance-management:fr-comp-009:fr-comp-009a`

The Statement addresses only generation of Security-Control Implementation Evidence for inclusion in a Security Control Traceability Matrix.

FR-COMP-009b governs Evidence generated for use in Risk Management Framework activities.

FR-COMP-009c governs Evidence generated for use in Authorization to Operate activities.

This requirement does not require Crucible to create, maintain, approve, or complete an SCTM.

Do not add Security Control approval, assessment authority, finding resolution, risk acceptance, or authorization responsibilities unless the controlling requirement changes through an approved requirements process.

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

```
{{section>dido:02-crusible:99-annexes:annex-c-requirements:03-functional-requirements:03-06-compliance-management:fr-comp-009:fr-comp-009a#Statement&noheader&nofooter&noeditbtn}}
```
