FR-COMP-009 — Security-Control Implementation Evidence

Go to Crucible Compliance Management Requirements

Original Requirement

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

Assessment of Original Requirement

The Original Requirement identifies three distinct uses for Security-Control Implementation Evidence:

1. Inclusion in a Security Control Traceability Matrix (SCTM)
2. Use in Risk Management Framework (RMF) activities
3. Use in Authorization to Operate (ATO) activities

Each use has a distinct purpose and requires separate verification. The Original Requirement should therefore be decomposed into three leaf requirements.

Generation of Security-Control Implementation Evidence is the common behavior across the three leaf requirements. It does not require a separate leaf because the Original Requirement does not establish an independent Evidence-generation obligation outside the SCTM, RMF, and ATO contexts.

The phrase **suitable for supporting** does not identify an observable behavior or the characteristics that make the Evidence suitable. Each child Statement therefore identifies the intended use directly.

The decomposition does not assign security-control approval, risk-management, risk-acceptance, authorization, or operational approval responsibilities to Crucible.

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.

Contents

Requirement Status

☐ Review and approve the decomposition of FR-COMP-009.

☐ Create and approve FR-COMP-009a.

☐ Create and approve FR-COMP-009b.

☐ Create and approve FR-COMP-009c.

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 separate requirements define the minimum content, identifiers, provenance, and references required for Security-Control Implementation Evidence.

☐ Determine which Evidence characteristics are required for inclusion in an SCTM.

☐ Determine which Evidence characteristics are required for use in RMF activities.

☐ Determine which Evidence characteristics are required for use in ATO activities.

Notes for Editors

This page is a non-leaf requirement page and therefore retains a trailing `:start` in 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:start`

The child requirements are leaf pages nested beneath the FR-COMP-009 namespace and omit a trailing `:start`.

Use the following controlling Terms and Definitions entries:

- Security Control Traceability Matrix (SCTM)
- Risk Management Framework (RMF)
- Authorization to Operate (ATO)
- Evidence

The decomposition contains three leaf requirements because the Original Requirement identifies three uses of Security-Control Implementation Evidence.

Do not create a separate generic Evidence-generation leaf unless the controlling source adds an independent requirement to generate Security-Control Implementation Evidence outside the SCTM, RMF, and ATO contexts.

FR-COMP-009 does not require Crucible to:

- Approve a Security Control implementation
- Perform the responsibilities of a control assessor
- Make a risk-management decision
- Accept residual risk
- Issue an Authorization to Operate
- Act as an Authorizing Authority

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