# FR-COMP-007 — Custom Compliance Frameworks

Go to Crucible Compliance Management Requirements

## Statement

Crucible SHALL define user-defined Compliance Frameworks.

## Derived From

This requirement derives from:

- Crucible System Requirements Specification, Version 1.1 Draft, Functional Requirements, FR-COMP-007

The Original Requirement states:

> *The system shall support custom compliance frameworks.*[C1]

FR-COMP-007:

- Replaces **The system** with the defined system name Crucible
- Changes **shall** to the established uppercase normative form **SHALL**
- Replaces the weak verb **support** with the observable behavior **define**
- Replaces the relative adjective **custom** with **user-defined**
- Preserves Compliance Framework as the source-identified subject

No other substantive normalization is required.

## Rationale

Organizations can operate under compliance obligations that extend beyond standardized frameworks such as Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and Federal Risk and Authorization Management Program (FedRAMP) baselines.

User-defined Compliance Frameworks allow an organization to represent compliance criteria derived from:

- Organizational policies
- Contractual obligations
- Program-specific requirements
- Mission-specific requirements

- Customer requirements
- Industry standards
- Regulatory obligations
- Local security policies
- Combinations of existing compliance frameworks

A user-defined Compliance Framework can organize:

- Compliance requirements
- Security controls
- Compliance criteria
- Control mappings
- Evaluation procedures
- Expected values
- Severity classifications
- Required Evidence
- References to source authorities
- Associated Compliance Baselines

This requirement establishes definition of user-defined Compliance Frameworks without prescribing:

- A particular Compliance Framework
- A particular source authority
- Import of an externally defined framework
- Mapping between Compliance Frameworks
- Application of a Compliance Framework
- Compliance scanning
- Compliance assessment
- Compliance reporting
- Evidence generation
- Framework approval
- Framework publication
- Framework version management

Separate requirements, architecture specifications, workflows, or policies define those subjects and behaviors.

# Applies To

This requirement applies to:

- Crucible
- User-defined Compliance Frameworks
- Compliance Framework definition operations

# Verification

Verification confirms that:

1. A set of user-specified compliance criteria is selected for testing
2. Crucible defines a Compliance Framework containing the selected compliance criteria
3. The resulting Compliance Framework can be identified
4. The compliance criteria contained in the resulting Compliance Framework can be determined
5. The resulting Compliance Framework is not restricted to a predefined DISA STIG or FedRAMP framework

## Referenced By

The following pages reference this requirement:

- 5.4 Assess Compliance
- 6.1 Construct and Assess the Environment
- 8.1 Select Compliance Criteria and Baselines
- Annex D: Requirements Traceability

## Implementation Status

Implemented and Verified

## Requirement Status

☐ Review and approve FR-COMP-007 as a leaf requirement.

---

## Issues

☐ Determine whether Compliance Framework requires a controlled definition in the shared Terms and Definitions corpus.

☐ Determine whether separate requirements govern importing, mapping, approving, publishing, and maintaining user-defined Compliance Frameworks.

☐ Determine whether separate requirements govern deriving Compliance Baselines from user-defined Compliance Frameworks.

---

## Notes for Editors

This requirement page retains the stable requirement identifier `FR-COMP-007`.

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

The Statement preserves the approved source intent by requiring Crucible to define user-defined Compliance Frameworks.

The Statement uses **user-defined** rather than **custom** because **custom** does not identify who establishes the framework or how the framework differs from a predefined framework.

Do not change **define** to **provide**, **import**, **maintain**, **apply**, **scan against**, or **assess against** unless the controlling requirement identifies that specific behavior.

Do not add framework mapping, approval, publication, version management, scanning, reporting, or Evidence-generation obligations 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-007#Statement&noheader&nofooter&noeditbtn}}
```

---