Compliance

Go up to Terms and Definitions

Discussion

Compliance is the condition of satisfying specified legal, regulatory, contractual, policy, standard, control, benchmark, or other applicable criteria.

A Compliance determination depends on the defined:

- Subject
- Applicable criteria
- Controlling sources
- Controlling source Versions
- Scope
- Operating context
- Assessment method
- Evidence
- Time of evaluation
- Applicable Authority

Compliance can apply to:

- A Candidate Solution
- A Distributed System
- A system
- A service
- A process
- An Organization
- An Actor
- A Node
- A Qualified Node
- A Node Set
- An artifact
- A Configuration
- A Test Environment
- An individual control
- Another subject governed by applicable criteria

A subject can comply with one set of criteria while failing to comply with another.

Applicable criteria can originate from:

- Requirements
- Laws
- Regulations
- Contracts

- Agreements
- Governance Policies
- Standards
- Specifications
- Controls
- Benchmarks
- Decisions of an applicable Authority
- Other controlling sources

A Compliance evaluation can result in a determination such as:

- Satisfied
- Not satisfied
- Partially satisfied
- Not applicable
- Not evaluated
- Inconclusive
- Another status established by the applicable criteria

The controlling source, Governance Policy, Validation Criteria, or Acceptance Criteria establishes the permitted Compliance determinations.

Compliance differs from Accreditation. Compliance establishes satisfaction of specified criteria, while Accreditation provides formal recognition within a defined scope and operating context.

Definition

condition of satisfying specified legal, regulatory, contractual, policy, standard, control, benchmark, or other applicable criteria

Source

Generalized from:

- Conformity assessment
- Governance
- Risk management
- Regulatory practice
- Security engineering
- Quality management

Specialized for:

- Crucible architecture and operations
- DIDO Reference Architecture
- DIDO Reference Implementation Conceptual Model
- DIDO-TE comparative evaluation and Validation

The original definition and its approved intent are preserved.

Note

Compliance is not an absolute property without a stated reference.

A Compliance claim should identify:

- The subject
- The applicable criteria
- The controlling source
- The controlling source Version
- The evaluation scope
- The operating context
- The assessment method
- The evaluation time
- The applicable Authority
- The supporting Evidence

Evidence supports a Compliance determination but does not by itself establish that the subject satisfies the applicable criteria.

Compliance differs from Evaluation Characteristic:

- An Evaluation Characteristic identifies a characteristic selected for measurement, observation, comparison, or evaluation
- Compliance identifies the condition of satisfying applicable criteria

A comparative evaluation can evaluate the Compliance of multiple Candidate Solutions, but Compliance does not become a Quality Characteristic solely because it participates in the evaluation.

Compliance differs from Security:

- Compliance concerns satisfaction of applicable criteria
- Security concerns protection of information, operations, and Resources according to applicable authorization and security constraints

A subject can satisfy specified security criteria while retaining security risks not addressed by those criteria.

A subject can implement effective security controls but fail Compliance because it does not satisfy an applicable documentation, authorization, reporting, retention, or Evidence obligation.

Compliance differs from a Verdict:

- Compliance identifies a condition relative to applicable criteria
- A Verdict records an evaluation assigned to a Test Result

Multiple Test Results and Verdicts can support one Compliance determination.

Compliance differs from a Validation Decision:

- Compliance identifies the condition of satisfying applicable criteria
- A Validation Decision records a determination produced by evaluating information against Validation Criteria

A Validation Decision can establish or support the Compliance status of a subject.

An approved exception, waiver, or deviation does not erase the underlying criterion. The Compliance record should preserve:

- The underlying criterion
- The approved exception, waiver, or deviation
- The approving Authority
- The approval period
- The approval conditions
- The supporting Evidence
- The applicable Provenance
- The applicable Traceability

Example

A Hardened Image satisfies the applicable requirements of a selected Security Technical Implementation Guide (STIG) profile at the time of assessment.

The Compliance claim applies to:

- The identified Hardened Image
- The selected STIG profile
- The STIG profile Version
- The recorded Configuration
- The assessment scope
- The assessment method
- The evaluation time
- The supporting Evidence

In a DIDO-TE comparative evaluation, three Candidate Solutions are evaluated against the same regulatory, security, retention, audit, interoperability, and Evidence-preservation criteria.

DIDO-TE preserves Traceability among each Candidate Solution, applicable criterion, controlling source, Test Definition, Test Result, Verdict, Compliance determination, and supporting Evidence.
