COMPLIANCE WORKING RECORD

Certification scope and expiry checker

Fictional sample. Requires tailoring and responsible review.

Document control

Field	Value
Organization	Not recorded
Document type	Certification scope and expiry checker
Document reference	27-certification-scope-and-expiry-checker
Jurisdiction	United States
Version	1
Status	Review has unresolved requirements
Prepared by	Customer prepared
Prepared on	October 22, 2026
Sources reviewed	October 8, 2026
Generated	October 22, 2026

Purpose and boundary

Compare customer-coded purchased-service requirements with collective current certificate scope for each supplier and purchase. Check issuer, certificate status, duplicate or inconsistent records, issue chronology, expiry, and renewal windows.

Mechanical review applies only to the supplied source and customer-approved rules. It does not authenticate evidence, determine legal applicability, approve closure or work, clear a party, submit a filing, or change a source system.

Document control

Field	Value
Tool identifier	27-certification-scope-and-expiry-checker
Specification version	1
Dataset method revision	2026-10-08.task-dataset-review.1
Engine	validator
Result status	Review has unresolved requirements

Structured inputs

Field	Value
Frozen review date	October 8, 2026
Approved policy and scope reference	Fictional approved policy v1. Fictional reviewer. Replace before use.
Expiry warning window in calendar days	30

Result

2 source rows checked. 2 unresolved rows, 1 policy exceptions, and 2 missing checklist records.

- Compare customer-coded purchased-service requirements with collective current certificate scope for each supplier and purchase. Check issuer, certificate status, duplicate or inconsistent records, issue chronology, expiry, and renewal windows.

- Method revision 2026-10-08.task-dataset-review.1.

- Frozen review date 2026-10-08.

- Approved rule Fictional approved policy v1. Fictional reviewer. Replace before use..

- Every source row is preserved. Missing checklist entries use an empty source-row pointer. Duplicate identities remain unresolved in every occurrence.

- Exact identifiers and checklist values are case-sensitive. Status comparisons ignore case where the displayed contract names a supported status. Surrounding whitespace in identifiers requires review.

- Amounts use exact scaled-integer arithmetic. No source values, dates, quantities, or original bytes are changed.

- Mechanical review applies only to the supplied source and customer-approved rules. It does not authenticate evidence, determine legal applicability, approve closure or work, clear a party, submit a filing, or change a source system.

Measure	Value
Source rows	2
Result rows	4
Unresolved	2
Policy exceptions	1
Missing checklist records	2

Unresolved items

- Missing source record. fictional-supplier. No eligible current certificate covers the purchased-service requirement Hosting

- Missing source record. fictional-supplier. No eligible current certificate covers the purchased-service requirement Recovery

- Row 3. fictional-supplier. Certificate expired before the frozen review date. Purchased service lacks eligible certificate coverage for Hosting, Recovery

Detailed results

Row	Reference	Result	Finding
2	fictional-supplier	Within selected rules	The supported administrative checks found no exception under the selected rules.
3	fictional-supplier	Review required	Certificate expired before the frozen review date. Purchased service lacks eligible certificate coverage for Hosting, Recovery
Not provided	fictional-supplier	Unresolved	No eligible current certificate covers the purchased-service requirement Hosting
Not provided	fictional-supplier	Unresolved	No eligible current certificate covers the purchased-service requirement Recovery

Row	Purchase reference	Certificate	Issuer
2	fictional-purchase-1	fictional-certificate-1	Fictional issuer
3	fictional-purchase-2	fictional-certificate-2	Fictional issuer
Not provided	fictional-purchase-2	Not provided	Not provided
Not provided	fictional-purchase-2	Not provided	Not provided

Row	Certificate status	Certified scope	Purchased service scope
2	Current	Hosting|Support	Hosting|Support
3	Current	Hosting	Hosting|Recovery
Not provided	Not provided	Not provided	Hosting|Recovery
Not provided	Not provided	Not provided	Hosting|Recovery

Row	Issue date	Expiry date	Days until expiry
2	January 1, 2026	January 1, 2027	85
3	January 1, 2026	October 7, 2026	-1
Not provided	Not provided	Not provided	Not provided
Not provided	Not provided	Not provided	Not provided

Row	Eligible for declared coverage	Covered requirements	Missing requirements
2	Yes	Hosting|Support	Not provided
3	No	Not provided	Hosting|Recovery
Not provided	No	Not provided	Hosting
Not provided	No	Not provided	Recovery

Assumptions

- No additional assumption was recorded.

Limitations

- Mechanical review applies only to the supplied source and customer-approved rules. It does not authenticate evidence, determine legal applicability, approve closure or work, clear a party, submit a filing, or change a source system.

Official sources

Source	Provision	Date	Link
National Institute of Standards and Technology: Cybersecurity Supply Chain Risk Management Practices, updated November 1, 2024	Supply chain risk strategy, controls, assessment and monitoring. This source supports the Certification scope and expiry checker scope described on this page. It does not determine applicability or approve the customer result.	October 8, 2026	https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final
US Government Accountability Office: Standards for Internal Control in the Federal Government	Five components, 17 principles and documentation attributes. This source supports the Certification scope and expiry checker scope described on this page. It does not determine applicability or approve the customer result.	September 24, 2026	https://www.gao.gov/greenbook