

COMPLIANCE WORKING RECORD

VEX record assembler

Fictional sample. Requires tailoring and responsible review.

Document control

Field	Value
Document type	VEX record assembler
Document reference	17-vex-record-assembler
Jurisdiction	United States
Version	2026-10-09.local-interchange.1
Status	Named review prepared
Prepared by	Fictional Responsible reviewer
Prepared on	October 9, 2026
Generated	October 9, 2026

Purpose and boundary

Assemble explicitly approved affected-status statements in OpenVEX 0.2.0 format.

Working results use exact local sources and explicitly selected versions. Originals remain unchanged in this browser. No source authenticity, population completeness, vulnerability exploitability, legal applicability, license conclusion, consent validity, food safety or external submission is established.

Method and exact sources

Method revision 2026-10-09.local-interchange.1.

Resolve exact product references and versions. Require explicit approved status, evidence and statement time. A not_affected statement needs an allowed justification or impact statement. An affected statement requires an action statement. Reject conflicting statuses for the same product, vulnerability and instant. Produce an OpenVEX 0.2.0 JSON document, retaining customer approval and source lineage separately. Statuses are supplied conclusions, not scanner-derived decisions.

Working results use exact local sources and explicitly selected versions. Originals remain unchanged in this browser. No source authenticity, population completeness, vulnerability exploitability, legal applicability, license conclusion, consent validity, food safety or external submission is established.

Source	Filename	Bytes	SHA-256
primary	fictional-observations.csv	383	b7e4de26463e6f32e4dc6329c6af8264e028f baf9c8e0abe5a5f5d9405bd0520
comparison	fictional-approved-rules.csv	123	9ca5046a47b9f654f8ba358159c0d610ef75 14180164238e89961a5280a38cf0

Frozen inputs

Field	Value
Review reference	Fictional Review reference
Responsible reviewer	Fictional Responsible reviewer
Observation date	October 9, 2026
Source and version scope	Fictional Source and version scope
VEX document IRI	https://example.invalid/fictional-vex/1
VEX document version	1
VEX issue timestamp	2026-10-09T12:00:00Z

Review result

3 source-linked findings. 0 unresolved or failed findings.

- Resolve exact product references and versions. Require explicit approved status, evidence and statement time. A not_affected statement needs an allowed justification or impact statement. An affected statement requires an action statement. Reject conflicting statuses for the same product, vulnerability and instant. Produce an OpenVEX 0.2.0 JSON document, retaining customer approval and source lineage separately. Statuses are supplied conclusions, not scanner-derived decisions.

- Original files are unchanged. Working artifacts are separate and withheld when their required checks fail.

Measure	Value
Original files	2
Working artifacts	1
Unresolved findings	0

VEX statement index

The first 25 working rows appear here. Each working preview is limited to 1000 characters. Complete rows and all exact source values remain in Excel and JSON.

Reference	Working result
STATEMENT1	statement id STATEMENT1; product id PRODUCT1; vulnerability id CVE-2026-00001; status not_affected; approval ref FICTIONAL-APPROVAL; source ref FICTIONAL-SOURCE

Source-linked checks

The formal report shows at most the first 100 named check rows and 400 characters per displayed field. Complete values, result columns, sources and output are retained in the Excel and JSON files.

Reference	Result	Finding
Primary / 2	Prepared	Customer status and approval linked to exact product/version and source evidence.

Unresolved items and limitations

- Working results use exact local sources and explicitly selected versions. Originals remain unchanged in this browser. No source authenticity, population completeness, vulnerability exploitability, legal applicability, license conclusion, consent validity, food safety or external submission is established.

Limitations

- Working results use exact local sources and explicitly selected versions. Originals remain unchanged in this browser. No source authenticity, population completeness, vulnerability exploitability, legal applicability, license conclusion, consent validity, food safety or external submission is established.

Official sources

Source	Provision	Date	Link
RFC Editor: Common Format and MIME Type for CSV Files	Supports CSV interchange only. It specifies no approved domain population, legal criterion or task decision.	October 9, 2026	https://www.rfc-editor.org/rfc/rfc4180
OpenVEX: OpenVEX Specification 0.2.0	Supports OpenVEX 0.2.0 structure. All impact conclusions and approvals are customer supplied and remain unverified.	October 9, 2026	https://github.com/openvex/spec/blob/main/OPENVEX-SPEC.md