

COMPLIANCE WORKING RECORD

CRA vulnerability reporting preparation

Fictional sample. Requires tailoring and responsible review.

Document control

Field	Value
Document type	CRA vulnerability reporting preparation
Document reference	FICTIONAL-INCIDENT-1
Jurisdiction	Customer-selected EU exercise scope
Version	1
Status	Named incident preparation pack prepared
Prepared by	Fictional responsible incident reviewer
Prepared on	2026-10-09T18:00:00Z
Rule pack	2026-10-09.incident-preparation.1
Generated	October 9, 2026

Purpose and boundary

Prepare product vulnerability and severe-incident reporting records from supplied exploitation and remediation evidence.

Link the exact manufacturer, product version, affected vulnerability versions, awareness event, exploitation evidence and available fix. Reconcile customer-selected operative reporting stages, recipient, fields, source version and approved clock basis. Flag mismatched products, incomplete fixes and conflicting stage records. No authority report is sent.

This working pack organizes customer-supplied incident facts, original evidence, approved rule versions and recorded decisions. It does not decide legal applicability, notification duties, statutory deadlines, insurance coverage, AI seriousness, product exploitation, authenticity or sanctions clearance. No report, message, authority filing or payment is sent. Original files remain unchanged and browser-local unless explicitly saved through paid private cloud saving.

Approved scope and incident preparation method

Fictional exercise only. Two confirmed supplied events and one selected approved duty where applicable. Replace every fact, rule and source before use.

Scope approval. FICTIONAL-SCOPE-1

Approved method. Fictional approved preparation procedure 1. Source. f1. Locator. /methodVersion. Approver. Fictional authorized procedure approver. Approval date. 2026-01-01T12:00:00Z

Population statement. Declared complete population. Customer-declared count. 2

Product vulnerability and reporting stage dossier event inputs

The first 20 exact task rows appear here. Displayed values are bounded to 1000 characters. Complete typed rows and exact values remain in Excel and JSON.

ID	Facts
1	Event ID. E1 Incident ID. FICTIONAL-INCIDENT-A Kind. Awareness Description. Fictional reviewer confirmed awareness of the selected incident. Event At. 2026-10-08T10:00:00-04:00 End At. Precision. Instant Certainty. Customer-confirmed Sequence After. [] Recorded At. 2026-10-08T14:05:00Z Reported By. Fictional incident observer Confirmed By. Fictional incident owner Source File ID. f2 Source Pointer. /events/0 Source Mode. Exact JSON record
2	Event ID. E2 Incident ID. FICTIONAL-INCIDENT-A Kind. Containment Description. Fictional selected system was isolated within this exercise scope. Event At. 2026-10-08T15:00:00Z End At. Precision. Instant Certainty. Customer-confirmed Sequence After. ["E1"] Recorded At. 2026-10-08T15:05:00Z Reported By. Fictional response operator Confirmed By. Fictional incident owner Source File ID. f2 Source Pointer. /events/1 Source Mode. Exact JSON record

Products

The first 20 exact task rows appear here. Displayed values are bounded to 1000 characters. Complete typed rows and exact values remain in Excel and JSON.

ID	Facts
1	Product ID. PR1 Product Version. 1.0 Manufacturer. Fictional Northfield Release At. 2026-01-01T12:00:00Z Vulnerability IDs. ["V1"] Exploitation State. Reported active exploitation Source File ID. f3 Source Pointer. /products/0 Source Mode. Exact JSON record Evidence IDs. ["PROOF-products-0"]

Vulnerabilities

The first 20 exact task rows appear here. Displayed values are bounded to 1000 characters. Complete typed rows and exact values remain in Excel and JSON.

ID	Facts
1	Vulnerability ID. V1 Identifier. FICTIONAL-VULNERABILITY-1 Affected Versions. ["1.0"] Discovered At. 2026-10-07T12:00:00Z Awareness Event ID. E1 Known Exploitation At. 2026-10-08T13:00:00Z Remediation State. Available Fixed Version. 1.1 Fix Available At. 2026-10-09T12:00:00Z Source File ID. f3 Source Pointer. /vulnerabilities/0 Source Mode. Exact JSON record Evidence IDs. ["PROOF-vulnerabilities-0"]

Duties

The first 20 exact task rows appear here. Displayed values are bounded to 1000 characters. Complete typed rows and exact values remain in Excel and JSON.

ID	Facts
1	Duty ID. D1 Incident ID. FICTIONAL-INCIDENT-A Instrument. Fictional approved incident reporting criteria Provision. Fictional exercise reporting stage 1 Rule Version. Fictional approved preparation procedure 1 Jurisdiction. Customer-selected EU exercise scope Entity Role. Fictional responsible organization Recipient. Fictional selected reporting recipient Stage. Initial working report Trigger Event ID. E1 Applicability. Applies Basis. Fictional customer-approved exercise assumption. No legal applicability conclusion. Approved By. Fictional authorized procedure approver Approved At. 2026-01-01T12:00:00Z Clock Mode. Elapsed hours Interval. 48 Explicit Due At. Trigger Date. Trigger Calendar Offset. Due Time. Due Offset. Calendar Basis. Business Weekdays. Excluded Dates. [] Count Start. Roll. None Predecessor Duty ID. Predecessor State. Supersedes ID. Report Field IDs. ["RF1"] Policy ID. System ID. Product ID. PR1 Source File ID. f3 Source Pointer. /duties/0 Source Mode. Exact [formal preview abridged]

Submissions

The first 20 exact task rows appear here. Displayed values are bounded to 1000 characters. Complete typed rows and exact values remain in Excel and JSON.

ID	Facts
1	Submission ID. S1 Duty ID. D1 Recipient. Fictional selected reporting recipient Stage. Initial working report Rule Version. Fictional approved preparation procedure 1 State. Prepared Prepared At. 2026-10-08T16:00:00Z Dispatched At. Acknowledged At. Receipt reference. Actor. Fictional reporting preparer Source File ID. f3 Source Pointer. /submissions/0 Source Mode. Exact JSON record Evidence IDs. ["PROOF-submissions-0"]

Report Fields

The first 20 exact task rows appear here. Displayed values are bounded to 1000 characters. Complete typed rows and exact values remain in Excel and JSON.

ID	Facts
1	Field ID. RF1 Duty ID. D1 Label. Fictional confirmed incident facts Value. Fictional incident awareness and containment were confirmed for the exact selected exercise scope. Event IDs. ["E1","E2"] Source File ID. f3 Source Pointer. /reportFields/0 Source Mode. Exact JSON record Evidence IDs. ["PROOF-reportFields-0"]

Evidence

The first 20 exact task rows appear here. Displayed values are bounded to 1000 characters. Complete typed rows and exact values remain in Excel and JSON.

ID	Facts
1	Evidence ID. PROOF-events-0 Record Type. events Record ID. E1 File ID. f2 Source Sha256. 34df952c0e7c3b900ee12de92fdf6eb648082b250940bf5ad464a36fcdf7c931 Locator. /events/0 Conclusion. Supports Reviewer. Fictional responsible source reviewer Reviewed At. 2026-10-09T17:00:00Z
2	Evidence ID. PROOF-events-1 Record Type. events Record ID. E2 File ID. f2 Source Sha256. 34df952c0e7c3b900ee12de92fdf6eb648082b250940bf5ad464a36fcdf7c931 Locator. /events/1 Conclusion. Supports Reviewer. Fictional responsible source reviewer Reviewed At. 2026-10-09T17:00:00Z
3	Evidence ID. PROOF-products-0 Record Type. products Record ID. PR1 File ID. f3 Source Sha256. fb2ffe8e1c8e8268b78db83134d560b143834800eb5cd52892b0adbe5ef2b8ca Locator. /products/0 Conclusion. Supports Reviewer. Fictional responsible source reviewer Reviewed At. 2026-10-09T17:00:00Z
4	Evidence ID. PROOF-vulnerabilities-0 Record Type. vulnerabilities Record ID. V1 File ID. f3 Source Sha256. fb2ffe8e1c8e8268b78db83134d560b143834800eb5cd52892b0adbe5ef2b8ca Locator. /vulnerabilities/0 Conclusion. Supports Reviewer. Fictional responsible source reviewer Reviewed At. 2026-10-09T17:00:00Z

ID	Facts
5	Evidence ID. PROOF-duties-0 Record Type. duties Record ID. D1 File ID. f3 Source Sha256. fb2ffe8e1c8e8268b78db83134d560b143834800eb5cd52892b0adbe5ef2b8ca Locator. /duties/0 Conclusion. Supports Reviewer. Fictional responsible source reviewer Reviewed At. 2026-10-09T17:00:00Z
6	Evidence ID. PROOF-submissions-0 Record Type. submissions Record ID. S1 File ID. f3 Source Sha256. fb2ffe8e1c8e8268b78db83134d560b143834800eb5cd52892b0adbe5ef2b8ca Locator. /submissions/0 Conclusion. Supports Reviewer. Fictional responsible source reviewer Reviewed At. 2026-10-09T17:00:00Z
7	Evidence ID. PROOF-reportFields-0 Record Type. reportFields Record ID. RF1 File ID. f3 Source Sha256. fb2ffe8e1c8e8268b78db83134d560b143834800eb5cd52892b0adbe5ef2b8ca Locator. /reportFields/0 Conclusion. Supports Reviewer. Fictional responsible source reviewer Reviewed At. 2026-10-09T17:00:00Z

Actions

The first 20 exact task rows appear here. Displayed values are bounded to 1000 characters. Complete typed rows and exact values remain in Excel and JSON.

Product vulnerability and reporting stage dossier

The first 20 prepared output rows appear here. Complete rows remain in Excel and JSON.

ID	Result
	Event ID. E1 Kind. Awareness Description. Fictional reviewer confirmed awareness of the selected incident. Original timestamp. 2026-10-08T10:00:00-04:00 Original interval end. UTC earliest. 2026-10-08T14:00:00Z UTC latest. 2026-10-08T14:00:00Z Elapsed span seconds. 0 Certainty. Customer-confirmed Source pointer. /events/0 Result. Normalized supplied interval
	Event ID. E2 Kind. Containment Description. Fictional selected system was isolated within this exercise scope. Original timestamp. 2026-10-08T15:00:00Z Original interval end. UTC earliest. 2026-10-08T15:00:00Z UTC latest. 2026-10-08T15:00:00Z Elapsed span seconds. 0 Certainty. Customer-confirmed Source pointer. /events/1 Result. Normalized supplied interval

Approved recipient and reporting stage matrix

The first 20 prepared output rows appear here. Complete rows remain in Excel and JSON.

ID	Result
	Duty ID. D1 Instrument. Fictional approved incident reporting criteria Provision. Fictional exercise reporting stage 1 Rule version. Fictional approved preparation procedure 1 Jurisdiction. Customer-selected EU exercise scope Entity role. Fictional responsible organization Recipient. Fictional selected reporting recipient Stage. Initial working report Applicability. Applies Trigger event ID. E1 Earliest cutoff. 2026-10-10T14:00:00Z Latest cutoff. 2026-10-10T14:00:00Z Assumptions. Elapsed hours after the supplied trigger interval. Exact elapsed units 48. Submission IDs. ["S1"] Result. Prepared for review

Product versions, vulnerabilities and remediation chronology

The first 20 prepared output rows appear here. Complete rows remain in Excel and JSON.

ID	Result
	Vulnerability ID. V1 Identifier. FICTIONAL-VULNERABILITY-1 Affected versions. ["1.0"] Discovery timestamp. 2026-10-07T12:00:00Z Awareness event ID. E1 Known exploitation timestamp. 2026-10-08T13:00:00Z Remediation state. Available Fixed version. 1.1 Fix availability timestamp. 2026-10-09T12:00:00Z Result. Source-linked vulnerability and remediation prepared

Owned incident response actions and dependencies

The first 20 prepared output rows appear here. Complete rows remain in Excel and JSON.

Named incident preparation draft sections

The first 20 prepared output rows appear here. Complete rows remain in Excel and JSON.

ID	Result

ID	Result
D1	<p>Item. D1 Decision. Prepared for review Draft text. Working report draft. Fictional selected reporting recipient. Initial working report</p> <p>Incident. FICTIONAL-INCIDENT-A. Organization. Fictional Northfield</p> <p>Operative customer-selected source. Fictional approved incident reporting criteria Fictional exercise reporting stage 1 Fictional approved preparation procedure 1. Jurisdiction. Customer-selected EU exercise scope. Role. Fictional responsible organization</p> <p>Fictional confirmed incident facts. Fictional incident awareness and containment were confirmed for the exact selected exercise scope.</p> <p>Approved trigger. E1. Elapsed hours after the supplied trigger interval. Exact elapsed units 48.</p> <p>This working pack organizes customer-supplied incident facts, original evidence, approved rule versions and recorded decisions. It does not decide legal applicability, notification duties, statutory deadlines, insurance coverage, AI seriousness, product exploitation, authenticity or sanctions clearance. [formal preview abridged]</p>

Incident preparation draft. D1. Prepared for review

Complete exact draft text remains in Excel and JSON.

Working report draft. Fictional selected reporting recipient. Initial working report

Incident. FICTIONAL-INCIDENT-A. Organization. Fictional Northfield

Operative customer-selected source. Fictional approved incident reporting criteria Fictional exercise reporting stage 1 Fictional approved preparation procedure 1. Jurisdiction. Customer-selected EU exercise scope. Role. Fictional responsible organization

Fictional confirmed incident facts. Fictional incident awareness and containment were confirmed for the exact selected exercise scope.

Approved trigger. E1. Elapsed hours after the supplied trigger interval. Exact elapsed units 48.

This working pack organizes customer-supplied incident facts, original evidence, approved rule versions and recorded decisions. It does not decide legal applicability, notification duties, statutory deadlines, insurance coverage, AI seriousness, product exploitation, authenticity or sanctions clearance. No report, message, authority filing or payment is sent. Original files remain unchanged and browser-local unless explicitly saved through paid private cloud saving.

Review findings

2 declared events. 1 exact approved duties. 0 unresolved findings.

The first 100 findings and 1000 characters per displayed field appear here. Complete findings remain in the data exports.

Kind	ID	Result	Finding
------	----	--------	---------

Kind	ID	Result	Finding
Original events source	E1	Matched	Every declared named fact matches the exact original JSON record.
Original events source	E2	Matched	Every declared named fact matches the exact original JSON record.
Original products source	PR1	Matched	Every declared named fact matches the exact original JSON record.
Original vulnerabilities source	V1	Matched	Every declared named fact matches the exact original JSON record.
Original duties source	D1	Matched	Every declared named fact matches the exact original JSON record.
Original submissions source	S1	Matched	Every declared named fact matches the exact original JSON record.
Original reportFields source	RF1	Matched	Every declared named fact matches the exact original JSON record.

Selected exact attachments

ID	Filename	Bytes	SHA-256
f1	fictional-approved-incident-procedure.json	264	cdc9180c17847fe0a77a157d594453fcf569c391061b829a01eb03aea00acb45
f2	fictional-original-incident-events.json	986	34df952c0e7c3b900ee12de92fdf6eb648082b250940bf5ad464a36fcdf7c931
f3	fictional-original-incident-task-records.json	2811	fb2ffe8e1c8e8268b78db83134d560b143834800eb5cd52892b0adb5ef2b8ca

Unresolved items and limitations

The first 100 unresolved items appear here, with 1000 characters per preview. Complete findings remain in Excel and JSON.

- This working pack organizes customer-supplied incident facts, original evidence, approved rule versions and recorded decisions. It does not decide legal applicability, notification duties, statutory deadlines, insurance coverage, AI seriousness, product exploitation, authenticity or sanctions clearance. No report, message, authority filing or payment is sent. Original files remain unchanged and browser-local unless explicitly saved through paid private cloud saving.

Limitations

- This working pack organizes customer-supplied incident facts, original evidence, approved rule versions and recorded decisions. It does not decide legal applicability, notification duties, statutory deadlines, insurance coverage, AI seriousness, product exploitation, authenticity or sanctions clearance. No report, message, authority filing or payment is sent. Original files remain unchanged and browser-local unless explicitly saved through paid private cloud saving.

Official sources

Source	Provision	Date	Link
European Union: Regulation (EU) 2024/2847. Cyber Resilience Act	Article 14, reporting of actively exploited vulnerabilities and severe incidents, and the applicable reporting stages. The customer supplies the operative version, product, manufacturer role, exploitation facts, recipient and approved clock basis. This workpaper neither establishes applicability nor transmits a report to ENISA or a CSIRT.. Link the exact manufacturer, product version, affected vulnerability versions, awareness event, exploitation evidence and available fix. Reconcile customer-selected operative reporting stages, recipient, fields, source version and approved clock basis. Flag mismatched products, incomplete fixes and conflicting stage records. No authority report is sent. No automated applicability, filing, authenticity or legal approval follows.	October 9, 2026	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847