PSD **Product Security Desk**

ILLUSTRATIVE CUSTOMER DELIVERABLE

CRA Reporting Readiness Report

A ten-business-day exercise of one product team's evidence, ownership and 24/72-hour reporting workflow.

ILLUSTRATIVE SAMPLE

Northwind Systems GmbH, EdgeControl Server, all release records, timings, findings, scores and recommendations are synthetic. CVE-2021-44228 is used only as a historical public exercise input.

MANUFACTURER Northwind Systems GmbH	**PRODUCT** EdgeControl Server
SCOPE One self-hosted product family: versions 4.8 LTS, 5.0 and 5.1	**ASSESSMENT DATE** 14 July 2026

EXECUTIVE VERDICT

The team can respond, but the process is not yet dependable.

The exercise produced a usable technical assessment within hours. It also exposed two blocked dependencies that could prevent a controlled notification workflow during a real event.

OVERALL READINESS

FRAGILE

The team assembled a usable package, but two evidence dependencies remained blocked.

AFFECTED-RELEASE STATEMENT

3h 15m

Versions 4.8 LTS and 5.0 were assessed as affected; 5.1 was assessed as not affected.

24-HOUR EVIDENCE

6 / 8

Operational inputs available by the exercise checkpoint.

72-HOUR EVIDENCE

11 / 14

Draft inputs available; sensitivity and release-level EU exposure were unresolved.

What requires management attention

BLOCKED G-01

EU availability cannot be resolved by affected release

The early-warning team cannot confidently identify the Member States in which affected releases were made available.

FRAGILE G-02

The supported 4.8 LTS dependency record is stale

Engineering had to reconstruct component exposure from build manifests during the reporting clock.

BLOCKED G-03

No owner can approve notification sensitivity after hours

The 72-hour package cannot be finalized without an improvised escalation path.

RECOMMENDED DECISION

Fund the first 30 days of the action plan before relying on this workflow for an actual reporting event. The priority is evidence ownership, not a new software platform.

EXERCISE DESIGN

A late-Friday component event tests the seams between teams.

The scenario starts outside normal working rhythm and requires product, release, customer and approval evidence to converge under time pressure.

TRIGGER

A customer reports evidence suggesting active exploitation of CVE-2021-44228 in a deployed EdgeControl Server instance late on a Friday.

Exercise assumptions

- The fictional manufacturer sells a self-hosted Java product into multiple EU Member States.
- The product has three supported release lines and appliance and container distributions.
- Customer indicators begin the assessment; the exercise does not make a legal determination that a report is required.
- No source code, binaries, credentials, customer-identifying data or non-public vulnerability information is used.
- Historical Log4Shell facts come from public CISA and Apache sources; all product mapping is synthetic.

Assessment questions

- Can the team identify affected supported releases and preserve the evidence?
- Can it assemble operational inputs used for a 24-hour early warning and 72-hour notification?
- Are decision rights, backups and escalation routes explicit enough to operate after hours?
- Can the manufacturer give users controlled mitigation guidance without overclaiming certainty?

CLOCK CONVENTION

Exercise elapsed time starts at Fri 16:10, when the fictional manufacturer first receives the customer report. This is an exercise convention, not a legal opinion on awareness.

PRODUCT BOUNDARY AND EVIDENCE

The current release is well evidenced; the LTS line is not.

Release-level traceability determines whether the team can move from a component alert to a defensible affected-product statement.

Supported release boundary

Release	Support	Component evidence	Exercise result	Status
4.8 LTS	Supported to Dec 2027	Dependency export dated 15 Sep 2025; build manifest available	Affected	FRAGILE
5.0	Maintenance	CycloneDX SBOM dated 20 Jun 2026; missing build hash	Affected	FRAGILE
5.1	Current	CycloneDX 1.5 SBOM bound to signed build hash	Not affected	READY

Evidence coverage

ID	Artifact	Owner	Date	Status
EV-01	Product and support policy	Release Engineering	2026-06-01	READY
EV-02	5.1 signed CycloneDX SBOM	Release Engineering	2026-07-10	READY
EV-03	5.0 CycloneDX SBOM	Release Engineering	2026-06-20	FRAGILE
EV-04	4.8 LTS dependency export	Former release owner	2025-09-15	BLOCKED
EV-05	EU customer availability export	Sales Operations	2026-07-11	BLOCKED
EV-06	PSIRT case PSIRT-1842	PSIRT	2026-07-13	READY
EV-07	Customer mitigation template	Support	2025-11-04	FRAGILE
EV-08	Notification decision log	PSIRT	2026-05-22	FRAGILE

INTERPRETATION

The 4.8 and 5.0 conclusions were reached, but not through the normal evidence path. That distinction is why both releases remain Fragile rather than Ready.

TABLETOP TIMELINE

A correct answer still consumed avoidable hours.

The timeline records when evidence appeared, where ownership failed and what remained unresolved at each checkpoint.

Time	Event	Owner	Evidence consequence
Fri 16:10	Customer support receives exploit indicators and a suspected product version.	Support	Clock start is not yet formally declared.
Fri 16:22	PSIRT acknowledges the case and records the awareness timestamp.	PSIRT	Awareness time preserved in PSIRT-1842.
Fri 16:48	5.0 SBOM identifies log4j-core 2.14.1.	Release Engineering	Affected component confirmed; build binding still unproven.
Fri 17:05	5.1 signed SBOM shows a non-affected component version.	Release Engineering	5.1 removed from the working affected set.
Fri 17:40	4.8 dependency owner is unavailable; the stored export is stale.	Release Engineering	Build manifests requested as fallback evidence.
Fri 18:55	Build manifests confirm log4j-core 2.14.1 in 4.8 and 5.0.	Engineering	Technical affected-release set completed.
Fri 19:25	VP Engineering approves the first affected-release statement.	VP Engineering	Elapsed time: 3h 15m.
Sat 09:30	Sales provides an EU customer export without installed-release data.	Sales Operations	Member-State exposure remains unresolved.
Sat 11:15	Support drafts release-specific user mitigation wording.	Support / PSIRT	Backup approval route is not documented.
Sat 15:50	24-hour package reaches 6 of 8 operational inputs.	PSIRT	EU release exposure and sensitivity approval remain blocked.
Mon 10:30	72-hour package reaches 11 of 14 operational inputs.	Response team	Package remains a draft pending two approvals.

MEASURED RESULT

The first affected-release statement was approved in 3h 15m. The 24-hour package remained incomplete because release-level EU availability and sensitivity approval could not be resolved.

24-HOUR READINESS

The early-warning path is technically fast but commercially blind.

The exercise team identified the product and vulnerability quickly. It could not connect affected releases to Member-State availability or complete the sensitivity approval path.

Operational input	Stage	Status	Evidence	Readiness note
Notification type and level	24h	READY	PSIRT-1842	Captured in the case template.
Manufacturer identity	24h	READY	Corporate profile	Approved legal entity and reporter details available.
Product identity	24h	READY	EV-01	Product family is clear; affected releases are supported by fallback evidence.
Member States where available	24h	BLOCKED	EV-05	Available by product family only, not affected release.
Notification title	24h	READY	PSIRT-1842	Concise working title approved.
CVE identifier	24h	READY	CVE-2021-44228	Historical public identifier used for the exercise.
Active-exploitation evidence	24h	FRAGILE	Customer indicators	Source is recorded; reliability decision criteria are not documented.
Awareness time and clock owner	24h	FRAGILE	PSIRT-1842	Timestamp exists; backup clock owner is not named.

5	2	1
READY	FRAGILE	BLOCKED

INTERPRETATION

The team can identify the manufacturer, product and vulnerability. The package is still commercially blind because affected-release availability by Member State cannot be produced.

IMPORTANT BOUNDARY

Status describes exercise readiness. It is not a legal conclusion about reportability, awareness or compliance.

72-HOUR AND FINAL-REPORT READINESS

The technical narrative is stronger than the approval record.

The later-stage package has useful technical content but cannot be finalized predictably without two decision controls.

Operational input	Stage	Status	Evidence	Readiness note
General nature of vulnerability	72h	READY	PSIRT assessment	Remote-code-execution scenario summary drafted.
General nature of exploit	72h	READY	Customer indicators	High-level exploit description available.
Corrective or mitigating measures taken	72h	READY	Engineering work item	Upgrade and temporary controls documented.
Measures users can take	72h	FRAGILE	EV-07	Draft exists but lacks backup approval.
Sensitivity classification	72h	BLOCKED	EV-08	No after-hours approver or documented criteria.
Initial severity and impact assessment	72h	FRAGILE	PSIRT assessment	Technical severity exists; customer impact is incomplete.
Corrective-measure availability date	Final	READY	Release ticket	Patch publication time can be evidenced.
Full severity and impact	Final	FRAGILE	Incident record	Requires customer-impact consolidation.
Malicious actor information, if available	Final	NOT ASSESSED	None	No actor attribution was attempted in the exercise.
Security-update details	Final	READY	Release notes	Version, hash, publication and installation guidance available.

5	3	1	1
READY	FRAGILE	BLOCKED	NOT ASSESSED

INTERPRETATION

Mitigation and update evidence are available. Customer impact, sensitivity and final approval still depend on manual consolidation.

WORKFLOW AND DECISION RIGHTS

Technical work is owned; material approvals are not resilient.

The RACI excerpt shows the primary route tested in the exercise. A customer version would also identify named backups and contact paths.

Decision or activity	Responsible	Accountable	Consulted	Informed
Declare awareness time	PSIRT Lead	VP Engineering	Support	Response team
Determine affected releases	Release Engineering	VP Engineering	PSIRT	Support / Sales
Assess exploitation evidence	PSIRT Lead	VP Engineering	Release Engineering	Response team
Identify EU availability	Sales Operations	Commercial Director	PSIRT	Response team
Approve sensitivity	Legal / Privacy	General Counsel	PSIRT / CISO	Response team
Approve user mitigation	Support Lead	VP Engineering	PSIRT / Product	Customers
Authorize notification	VP Engineering	Managing Director	Legal / PSIRT	Response team
Preserve submitted evidence	PSIRT Coordinator	PSIRT Lead	IT / Legal	Audit owner

Decision-control observations

- The PSIRT Lead records the case, but the awareness-clock backup is not defined.
- VP Engineering can authorize the technical statement; notification authority has only one backup.
- Sensitivity approval depends on Legal / Privacy, with no documented after-hours substitute.
- Sales Operations owns availability evidence but does not capture installed release data.

CONTROL PRINCIPLE

Material regulatory, exploitability, sensitivity and disclosure judgments require qualified human review and explicit manufacturer approval.

PRIORITY GAP REGISTER

Six gaps explain nearly all of the exercise friction.

Each gap is tied to an operational consequence, an accountable owner and a target window. The register is deliberately short enough to manage.

ID	Status	Gap	Operational consequence	Owner	Target
G-01	BLOCKED	EU availability is not recorded by installed release.	24-hour Member-State input may be incomplete.	Sales Operations	15 days
G-02	FRAGILE	4.8 LTS has no current build-bound SBOM.	Affected-release analysis depends on manual reconstruction.	Release Engineering	30 days
G-03	FRAGILE	The clock owner has no named backup.	A late or ambiguous awareness declaration could compress the response window.	PSIRT Lead	15 days
G-04	BLOCKED	Sensitivity approval has no after-hours route.	The 72-hour package cannot be finalized predictably.	General Counsel	15 days
G-05	FRAGILE	User mitigation wording lacks a backup approver.	Customer instructions may be delayed during an event.	Support Lead	30 days
G-06	FRAGILE	Evidence links are split across three repositories.	Review and handover are slower and harder to audit.	PSIRT Coordinator	60 days

Blocked

A decision or evidence path could not complete without improvisation.

Fragile

The result depended on stale evidence, one-person knowledge or an unapproved fallback.

Ready

Current, traceable evidence was produced through the intended owner and workflow.

NO READINESS PERCENTAGE

A single percentage would hide which dependency blocks the workflow. Status is assessed field by field and linked to evidence instead.

NINETY-DAY ACTION PLAN

Fix ownership and traceability before adding tooling.

The sequence prioritizes changes that remove blocked decisions and make the next exercise measurable.

ID	Window	Action	Owner	Acceptance evidence	Gap
A-01	0-15	Name the reporting clock owner, backup and awareness trigger.	PSIRT Lead	Approved responsibility and escalation record	G-03
A-02	0-15	Create an after-hours sensitivity and notification approval route.	General Counsel	Decision criteria plus primary and backup approvers	G-04
A-03	0-15	Add installed-release and Member-State fields to the EU availability export.	Sales Operations	Queryable release-level distribution register	G-01
A-04	16-30	Regenerate 4.8 LTS and 5.0 SBOMs and bind them to release hashes.	Release Engineering	Signed build-bound CycloneDX SBOMs	G-02
A-05	16-30	Approve user mitigation templates and a backup approval path.	Support Lead	Release-specific customer notice workflow	G-05
A-06	31-60	Create one evidence index linking each supported release to source artifacts.	PSIRT Coordinator	Versioned evidence index with owners and dates	G-06
A-07	61-90	Run a second tabletop using a severe-incident scenario.	PSIRT Lead	Measured exercise record and updated runbook	All
A-08	61-90	Test SRP access and data entry when the official environment is available.	PSIRT Coordinator	Recorded dry run; no official submission	All

FIRST MANAGEMENT CHECKPOINT

By day 15, confirm A-01 through A-03: clock ownership, approval coverage and release-level EU availability. These are the prerequisites for a more reliable 24-hour package.

REPORTING RUNBOOK EXCERPT

Eight controlled steps from awareness to closure.

This excerpt demonstrates the handover format. A customer runbook would include named contacts, repositories, approval gates and customer-specific evidence locations.

Step	Control point	Action	Primary owner	Target
1	Open and preserve	Record awareness source and timestamp; create the case and immutable evidence index.	PSIRT Coordinator	15 min
2	Classify the event	Separate vulnerability and incident paths; escalate material judgments for qualified review.	PSIRT Lead	45 min
3	Bound product exposure	Identify supported releases, component versions, deployment models and available EU exposure evidence.	Release Engineering	2 h
4	Assemble 24-hour inputs	Prepare identity, product, availability, title, exploitation basis and clock evidence.	PSIRT Coordinator	8 h
5	Approve early warning	Resolve sensitivity, notification authority and any unresolved evidence statements.	VP Engineering / Legal	20 h
6	Complete 72-hour assessment	Add vulnerability or incident nature, initial impact, mitigations and user actions.	Response team	60 h
7	Submit or record no-submit decision	Manufacturer-approved action only; preserve the submitted content and receipt.	Authorized manufacturer	Before deadline
8	Maintain final-report record	Track update availability, full impact, root cause or actor information, and ongoing mitigations.	PSIRT Lead	Until closure

APPROVAL GATE

No official submission or external vulnerability disclosure is automated by this runbook. The manufacturer must authorize the action and the exact content.

METHOD, LIMITATIONS AND SOURCES

Traceable enough to review; bounded enough to deliver.

This sample shows the expected structure and evidence discipline. It is not a customer assessment and does not establish CRA scope, reportability or compliance.

Method

- Define one product and supported-release boundary.
- Review available SBOM, release, vulnerability, commercial and governance evidence.
- Run one timed tabletop and preserve evidence used at each decision point.
- Map exercise outputs to current official reporting information categories.
- Record gaps, owners, acceptance evidence and a sequenced ninety-day plan.
- Submit material conclusions to independent expert review.

Limitations

The sprint does not provide legal advice, a binding scope opinion, certification, conformity assessment, CE marking, source-code review, penetration testing, remediation implementation, an official filing or a compliance guarantee.

CUSTOMER HANDOVER

Executive report, evidence matrix, reporting runbook, gap register, responsibility map, ninety-day plan and final presentation.

Authoritative and technical sources

1. **EU Cyber Resilience Act, Article 14**
   Reporting stages and statutory information categories.
   https://eur-lex.europa.eu/eli/reg/2024/2847/oj?locale=en
2. **ENISA Single Reporting Platform FAQ**
   Current reporting-field matrix and platform implementation information.
   https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp
3. **European Commission CRA reporting guidance**
   Current reporting sequence and application date.
   https://digital-strategy.ec.europa.eu/en/policies/cra-reporting
4. **CISA Log4Shell advisory**
   Historical public exercise facts for CVE-2021-44228.
   https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a
5. **Apache Log4j release notes**
   Historical remediation and release information.
   https://logging.apache.org/log4j/2.x/release-notes.html