SYNTERA
SYSTEMS

REPORTING OBLIGATIONS BEGIN
SEPT. 11, 2026

EU CYBER RESILIENCE ACT

24/72-HOUR REPORTING READINESS & EVIDENCE SYSTEM

Excel-based control system for preparing CRA vulnerability and severe-incident reports through the ENISA Single Reporting Platform.

Prepare. Report. Document. Defend.

Workbook + implementation guide + emergency runbook

SELECTED WORKBOOK PREVIEW

CURRENT THROUGH SEPTEMBER 3, 2026 - SYNTHETIC EXAMPLES ONLY

24 — 24-HOUR CONTROL
Early-warning packet
Track awareness and due time

72 — 72-HOUR CONTROL
Full notification
Build the expanded record

FINAL REPORT
Remediation evidence
Document root cause and fix

SUBMISSION PROOF
Confirmation evidence
Preserve exact submitted content

A 20-tab control system for the reporting clock

The workbook connects setup, event control, stage-specific preparation, submission proof, and evidence preservation in one operating file.

01 ORIENT	02 DECIDE	03 CONTROL	04 EVIDENCE	05 ALIGN
Lists	Event Intake	Submission Log	Evidence Register	SRP Field Map
START HERE	Trigger Assessment	Reporting Timeline	Tabletop Exercise	Worked Examples
Company Setup	Notification Data	Corrective Measures	24-Hour Packet	Regulatory Reference
Product Register		User Communications	72-Hour Packet	Dashboard
			Final Report	
4	3	4	5	4

CONTROL PATH

Start with a controlled operating workflow

The START HERE tab defines scope, deadlines, roles, workbook conventions, and a ten-step implementation path before a real event occurs.

SYNTERA EU CYBER RESILIENCE ACT 24/72-HOUR REPORTING READINESS & EVIDENCE SYSTEM

Pre-launch edition v1.0 | September 2026 | Built around the ENISA Single Reporting Platform guidance updated 31 August 2026

PURPOSE

A controlled Excel system for preparing, managing, documenting, and supporting notifications of actively exploited vulnerabilities and severe incidents under the EU Cyber Resilience Act. The workbook is designed to help manufacturers and open-source software stewards organize internal facts before entering them into ENISA's Single Reporting Platform (SRP).

SCOPE BOUNDARY

This workbook is an operational readiness, evidence, deadline, and document-control aid. It does not determine whether a product or occurrence is legally in scope; make a binding determination that a vulnerability is actively exploited or that an incident is severe; provide cybersecurity engineering, incident response, legal advice, or regulatory representation; submit a notification; replace ENISA's SRP; or guarantee compliance. Users must verify current law and ENISA guidance and obtain qualified legal or cybersecurity advice when facts are uncertain or consequences are material.

10-STEP OPERATING WORKFLOW

Step	Control	Action
1	Set up company and SRP roles	Complete Company Setup, record the Article 14(7) CSIRT routing basis, and assign SRP Primary/Secondary Assigned Representatives (platform users). These platform roles are distinct from a CRA Article 18 authorised
2	Build the product register	Record products, versions, EU availability, support information, product owners, and evidence locations.
3	Capture the first signal	Create an Event Intake record as soon as a credible report, alert, supplier notice, or internal finding arrives.
4	Document awareness	After a prompt initial assessment, record the earliest UTC time at which the manufacturer had a reasonable degree of certainty that active exploitation or a severe incident meeting the CRA trigger existed; preserve the factual basis. A signal alone is not necessarily awareness, and internal approval cannot postpone this time.
5	Assess the trigger	Use Trigger Assessment to organize facts; escalate uncertain or potentially reportable events immediately.
6	Start the clock	Use Reporting Timeline to monitor the 24-hour and 72-hour deadlines and the event-specific final-report deadline.
7	Build the notification data	Populate Notification Data once. Use the same SRP notification record for the 24-hour early warning, 72-hour notification, subsequent updates, and final report. A draft is visible only to its creator, so plan handoffs in the controlled internal packet. After Final Report, the SRP record is non-editable.
8	Manage mitigation and communication	Track corrective measures, user actions, communications, and supporting evidence.
9	Preserve submissions	Log each submission and update, notification ID, confirmation email or alert, screenshot or export if available, exact submitted content, reviewer, and evidence link in Submission Log.
10	Test the process	Run Tabletop Exercise before an emergency and close all identified gaps.

KEY RULE FACTS

Reporting start	11 September 2026
Early warning	Without undue delay; no later than 24 hours after awareness
72-hour notification	Without undue delay; no later than 72 hours after awareness
AEV final report	No later than 14 days after a corrective or mitigating measure is available
Severe incident final report	Within one month after submission of the 72-hour incident notification
Platform	ENISA Single Reporting Platform
Time standard	Use UTC throughout this workbook
Transition scope	Article 14 reporting starts 11 Septembe 2026 for all in-scope products, includin earlier placements and products after support ends. Active exploitation alrea known before that date is not retroacti reportable solely because the date arr exploitation first learned afterward ca trigger reporting.
Conditional intermediate report	A coordinating CSIRT may request an intermediate report where necessary. its instructions and the live platform; t not a routine reporting stage.

WORKBOOK CONVENTIONS

Blue cells	User-entered facts or selections.
Green cells	Formula-driven or automatically populated information.
UTC timestamps	Enter date and time in UTC; do not mix local time zones in a live event record.
Evidence IDs	Use document IDs or secure links. Do not embed sensitive evidence in the workbook unless your security policy permits it.
Example data	The Worked Examples tab is illustrative only. Operational tabs are intended for your records.
Calculation timestamp	Update Company Setup!B19 with the current UTC date/time before relying on countdowns or status labels. Manual UTC entry avoids accidental use of a local computer time zone.

OFFICIAL SOURCES - VERIFY BEFORE USE

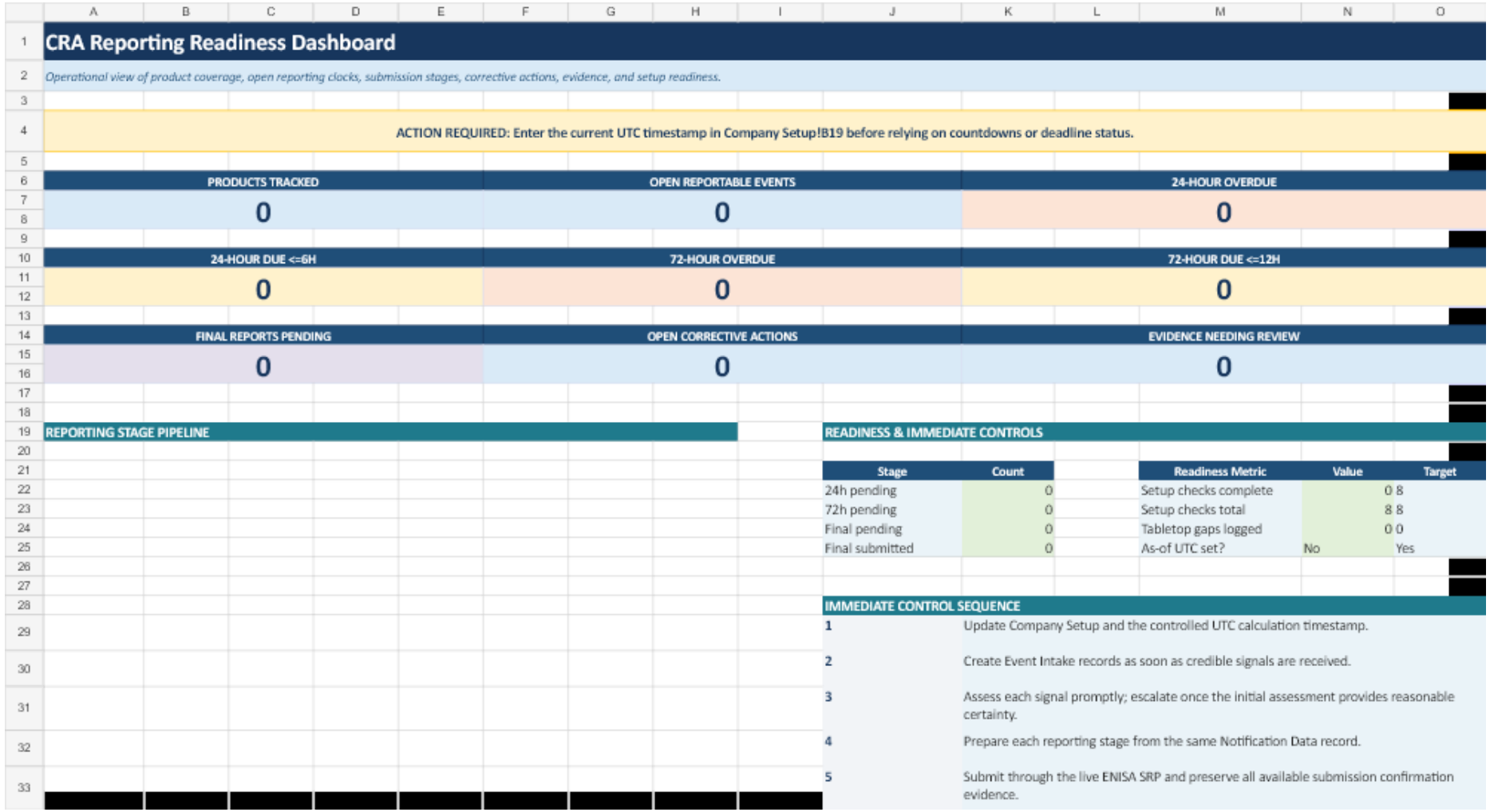
CRA policy	https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
CRA reporting	https://digital-strategy.ec.europa.eu/en/policies/cra-reporting
CRA summary	https://digital-strategy.ec.europa.eu/en/policies/cra-summary
ENISA SRP	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp
ENISA SRP FAQ	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
EU regulation	https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

READINESS PATH

1. **Configure**
   Name the reporting entity, roles, backups, and approval path.
2. **Register products**
   Record the product identity, ownership, EU availability, and evidence location.
3. **Preserve the first signal**
   Create the event record when a credible report, alert, supplier notice, or internal finding arrives.
4. **Record awareness**
   After prompt initial assessment, record the earliest reasonable-certainty UTC time and factual basis.
5. **Prepare and retain**
   Control stage facts, approval, notification IDs, platform confirmations, timestamps, and linked evidence.
6. **Exercise**
   Run fictional vulnerability and severe-incident scenarios before the clock is live.

See readiness, deadlines, and exceptions in one view

Fresh template state shown. Operational cards populate from configured records; the preview contains no customer data.



CRA Reporting Readiness Dashboard

Operational view of product coverage, open reporting clocks, submission stages, corrective actions, evidence, and setup readiness.

ACTION REQUIRED: Enter the current UTC timestamp in Company Setup!B19 before relying on countdowns or deadline status.

PRODUCTS TRACKED	OPEN REPORTABLE EVENTS	24-HOUR OVERDUE
0	0	0

24-HOUR DUE <=6H	72-HOUR OVERDUE	72-HOUR DUE <=12H
0	0	0

FINAL REPORTS PENDING	OPEN CORRECTIVE ACTIONS	EVIDENCE NEEDING REVIEW
0	0	0

REPORTING STAGE PIPELINE

Stage	Count
24h pending	0
72h pending	0
Final pending	0
Final submitted	0

READINESS & IMMEDIATE CONTROLS

Readiness Metric	Value	Target
Setup checks complete	0	8
Setup checks total	8	8
Tabletop gaps logged	0	0
As-of UTC set?	No	Yes

IMMEDIATE CONTROL SEQUENCE

1	Update Company Setup and the controlled UTC calculation timestamp.
2	Create Event Intake records as soon as credible signals are received.
3	Assess each signal promptly; escalate once the initial assessment provides reasonable certainty.
4	Prepare each reporting stage from the same Notification Data record.
5	Submit through the live ENISA SRP and preserve all available submission confirmation evidence.

Set roles and product records before an event

Blank controlled-entry areas keep entity, representative, backup, approval, product, support-period, and evidence-location facts ready for use.

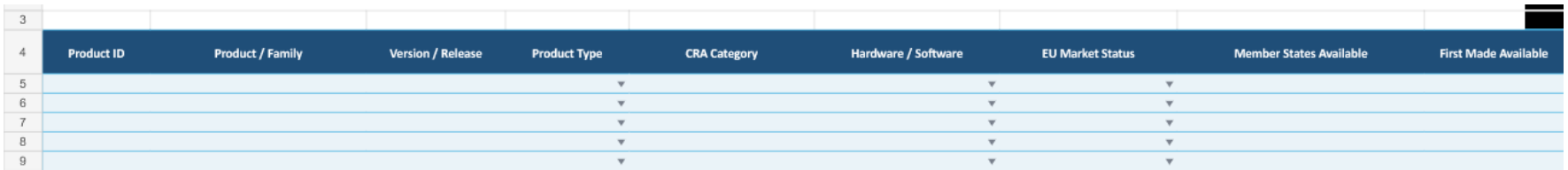
COMPANY SETUP

ORGANIZATION PROFILE	
Entity type	
Legal name	
Trading name	
Main establishment country	
Main establishment address	
Non-EU manufacturer?	
EU authorised representative	
Authorised representative country	
Selected CSIRT designated as coordinator	
Primary vulnerability-reporting contact	
24/7 escalation contact	
Standard workbook time zone	UTC
Last setup review date	
Setup owner	
Workbook calculation timestamp UTC	
[redacted]	[redacted]

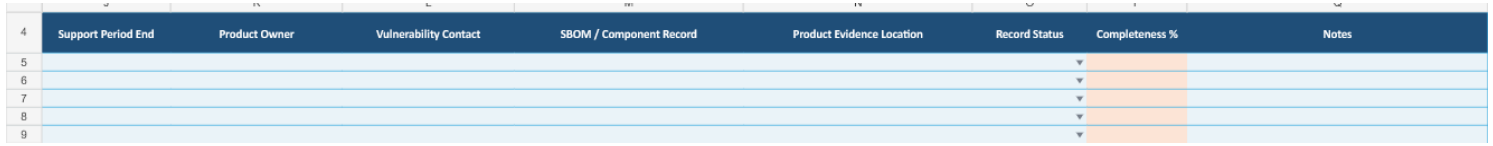
SRP ASSIGNED REPRESENTATIVE & INTERNAL ROLE REGISTER

Role ID	Name	Role / Function	Primary or Backup	Email	EU Login Ready?	2FA Ready?	Approval Authority	Notes

PRODUCT REGISTER - SELECTED COLUMNS



Product ID	Product / Family	Version / Release	Product Type	CRA Category	Hardware / Software	EU Market Status	Member States Available	First Made Available



Support Period End	Product Owner	Vulnerability Contact	SBOM / Component Record	Product Evidence Location	Record Status	Completeness %	Notes

Workbook convention Blue cells support controlled user entry; green cells present calculated or automated control output.

Set the clock from a documented reasonable-certainty assessment

Event Intake keeps the first signal separate from the earliest UTC time at which prompt initial assessment establishes reasonable certainty of a CRA trigger.

EVENT INTAKE - SELECTED COLUMNS

Event ID	Product ID	Event Type	Event Title	Source / Reporter	First Signal UTC	Awareness UTC	Awareness Assessment Owner	Reportability Decision	Decision Date UTC

Event Owner	Current Stage	24h Due UTC	72h Due UTC	Hours to 24h	Hours to 72h	Clock Status	Priority	External Advice?	Notes

REPORTING TIMELINE - SELECTED COLUMNS

Event ID	Event Type	Event Title	Awareness UTC	24h Due UTC	24h Submitted UTC	24h Status	72h Due UTC	72h Submitted UTC	72h Status

Corrective / Mitigating Measure Available UTC	Final Due UTC	Final Submitted UTC	Final Status	Next Deadline UTC	Next Action	Event Owner	PEC Review?	Notes

Reviewable clock

First signal, assessment owner, reasonable-certainty awareness time, due dates, stage status, and next action remain distinct.

Enter facts once; prepare each reporting stage

Notification Data holds common facts plus event-specific vulnerability or severe-incident detail. These are selected column groups, not the full worksheet.

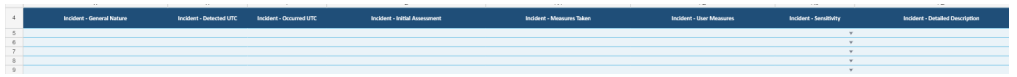
COMMON NOTIFICATION FIELDS - SELECTED

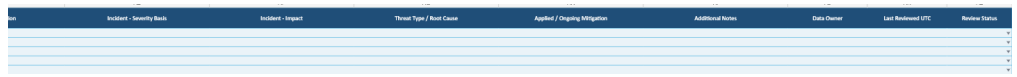
Event ID	Notification Type	Manufacturer / OSS Steward	Product	Product Type	Product Category	Member States Available

VULNERABILITY FIELDS - SELECTED

Vulnerability - Measures Taken	Vulnerability - User Measures	Vulnerability - Sensitivity	Corrective / Mitigating Measure Available UTC	Vulnerability - Full Description	Vulnerability - Severity

SEVERE-INCIDENT FIELDS - SELECTED GROUPS





Controlled preparation, not a portal replacement

The editable system supports internal preparation and review. Submission still occurs through the live ENISA Single Reporting Platform.

Prepare the 24-hour record before opening the portal

The copy-ready packet assembles the internal early-warning record and keeps review evidence next to the facts used for submission.

	A	B	C	D
1	**24-Hour Early Warning Packet**			
2	*Copy-ready internal preparation form for the CRA early warning stage.*			
3	Selected Event ID		Stage Due UTC	
4			Stage Status	
5				
6	SRP PACKET FIELDS			
7	Field	Controlled Value	Requirement at This Stage	Completion
8	Notification Type		Required	
9	Manufacturer / OSS Steward		Required	
10	Product		Required	
11	Product Type		Optional	
12	Product Category		Optional	
13	Member States Available		If available	
14	Notification Title		Required	
15	CVE ID		Optional	
16	EUVD ID		Optional	
17	Vulnerability - General Nature		Optional	
18	Exploit - General Nature		Optional	
19	Vulnerability - Measures Taken		Optional	
20	Vulnerability - User Measures		Optional	
21	Vulnerability - Sensitivity		Optional	
22	Incident - Suspected Unlawful / Malicious Acts?		Required if Severe Incident	
23	Incident - General Nature		Optional	
24	Incident - Detected UTC		Optional	
25	Incident - Occurred UTC		Optional	
26	Incident - Initial Assessment		Optional	
27	Incident - Measures Taken		Optional	
28	Incident - User Measures		Optional	
29	Incident - Sensitivity		Optional	
30				
31	PRE-SUBMISSION CONTROL CHECKLIST			
32	Control	Owner / Evidence	Status	
33	Awareness timestamp and 24-hour due time independently confirmed			
34	Notification type and product identity verified			
35	Member States information reviewed and entered if available			
36	Sensitive information / PEC escalation considered			
37	Designated internal reviewer completed the required review (or emergency override was documented)			
38	Assigned representative has SRP access and EU Login / 2FA			
39	Submission and confirmation evidence will be logged immediately			
40				
41	*Use this internal preparation aid. The SRP Assigned Representative (platform user) submits through ENISA's live SRP and preserves the notification ID, confirmation email or alert, screenshot or export if available, and exact submitted content in Submission Log.*			
42				
43				

Required focus

Reporting entity, product, notification type, reasonable-certainty awareness time, known identifiers, affected Member States if available, and high-level nature of the occurrence.

Internal control

Track draft ownership, approver, supporting evidence, sensitivity, and the factual basis used at the 24-hour stage.

Final check

Re-check the live SRP fields and current official instructions before each production submission.

Preserve submissions and the evidence behind them

Selected Submission Log and Evidence Register views connect each stage to ownership, confirmation evidence, supporting records, custody, retention, and review status.

SUBMISSION LOG - SELECTED COLUMNS

Lookup Key	Submission ID	Event ID	Stage	Draft Owner	Approver	Submitted By	Submitted UTC

Platform Notification ID	Confirmation Evidence ID / Link	CSIRT Designated as Coordinator	PEC Invoked?	Sensitivity	Evidence ID	Status	Notes

EVIDENCE REGISTER

Evidence Register

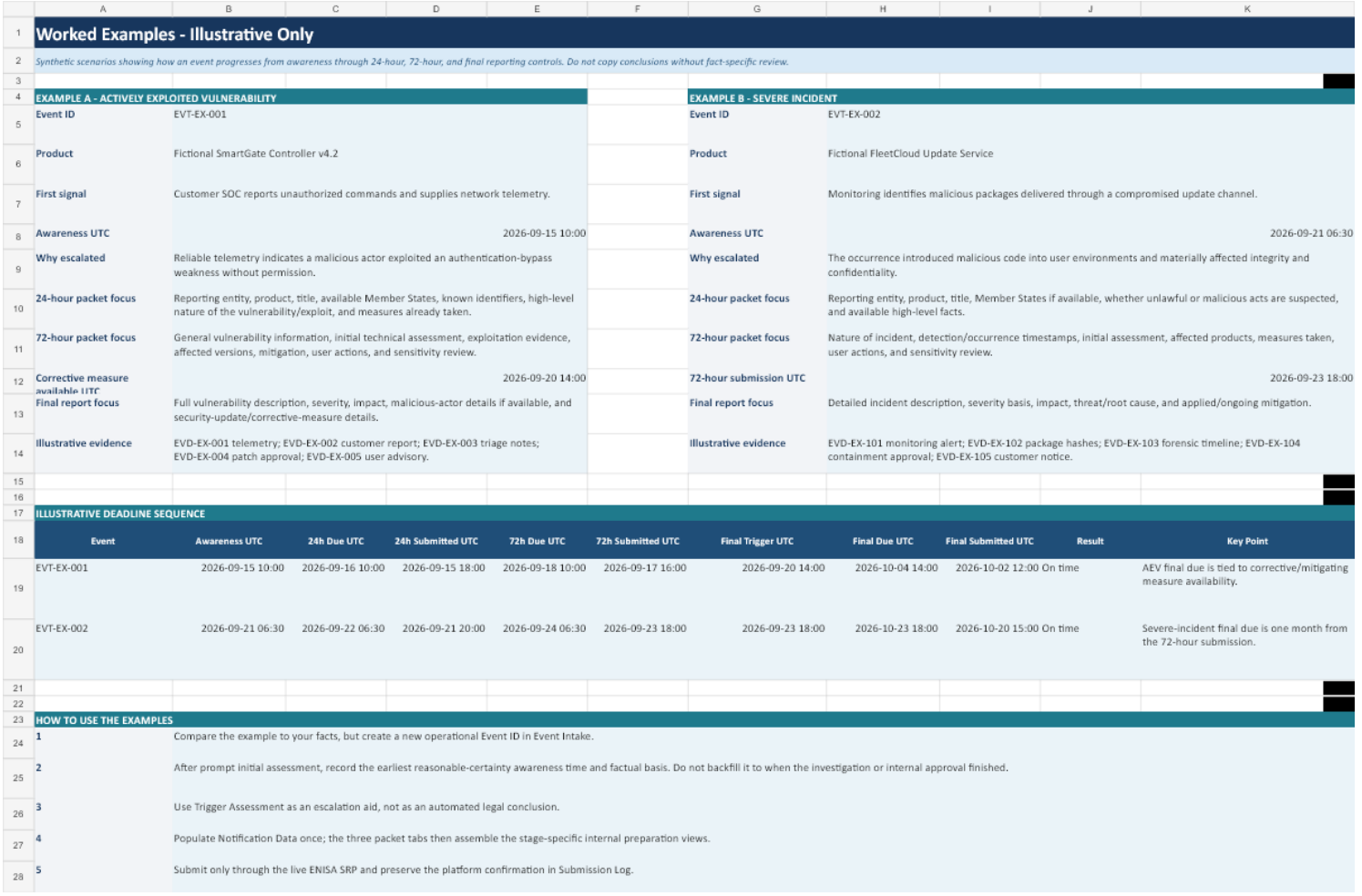
Index the facts and records supporting awareness, reportability decisions, notifications, measures, communications, and closure.

Evidence ID	Event ID	Product ID	Evidence Type	Description	Source / Origin	Created / Received UTC	Custodian	Secure Location / Link	Version / Hash	Sensitivity	Retention / Preservation Status	Review Status	Notes

Preserve the trail Notification ID, confirmation evidence, submitter, timestamp, evidence ID, custodian, secure location, version or hash, and review status.

Practice with fictional worked examples

The workbook includes illustrative scenarios so teams can rehearse the control path without using customer or production-event data.



Worked Examples - Illustrative Only

Synthetic scenarios showing how an event progresses from awareness through 24-hour, 72-hour, and final reporting controls. Do not copy conclusions without fact-specific review.

EXAMPLE A - ACTIVELY EXPLOITED VULNERABILITY

Event ID	EVT-EX-001
Product	Fictional SmartGate Controller v4.2
First signal	Customer SOC reports unauthorized commands and supplies network telemetry.
Awareness UTC	2026-09-15 10:00
Why escalated	Reliable telemetry indicates a malicious actor exploited an authentication-bypass weakness without permission.
24-hour packet focus	Reporting entity, product, title, available Member States, known identifiers, high-level nature of the vulnerability/exploit, and measures already taken.
72-hour packet focus	General vulnerability information, initial technical assessment, exploitation evidence, affected versions, mitigation, user actions, and sensitivity review.
Corrective measure available UTC	2026-09-20 14:00
Final report focus	Full vulnerability description, severity, impact, malicious-actor details if available, and security-update/corrective-measure details.
Illustrative evidence	EVD-EX-001 telemetry; EVD-EX-002 customer report; EVD-EX-003 triage notes; EVD-EX-004 patch approval; EVD-EX-005 user advisory.

EXAMPLE B - SEVERE INCIDENT

Event ID	EVT-EX-002
Product	Fictional FleetCloud Update Service
First signal	Monitoring identifies malicious packages delivered through a compromised update channel.
Awareness UTC	2026-09-21 06:30
Why escalated	The occurrence introduced malicious code into user environments and materially affected integrity and confidentiality.
24-hour packet focus	Reporting entity, product, title, Member States if available, whether unlawful or malicious acts are suspected, and available high-level facts.
72-hour packet focus	Nature of incident, detection/occurrence timestamps, initial assessment, affected products, measures taken, user actions, and sensitivity review.
72-hour submission UTC	2026-09-23 18:00
Final report focus	Detailed incident description, severity basis, impact, threat/root cause, and applied/ongoing mitigation.
Illustrative evidence	EVD-EX-101 monitoring alert; EVD-EX-102 package hashes; EVD-EX-103 forensic timeline; EVD-EX-104 containment approval; EVD-EX-105 customer notice.

ILLUSTRATIVE DEADLINE SEQUENCE

Event	Awareness UTC	24h Due UTC	24h Submitted UTC	72h Due UTC	72h Submitted UTC	Final Trigger UTC	Final Due UTC	Final Submitted UTC	Result	Key Point
EVT-EX-001	2026-09-15 10:00	2026-09-16 10:00	2026-09-15 18:00	2026-09-18 10:00	2026-09-17 16:00	2026-09-20 14:00	2026-10-04 14:00	2026-10-02 12:00	On time	AEV final due is tied to corrective/mitigating measure availability.
EVT-EX-002	2026-09-21 06:30	2026-09-22 06:30	2026-09-21 20:00	2026-09-24 06:30	2026-09-23 18:00	2026-09-23 18:00	2026-10-23 18:00	2026-10-20 15:00	On time	Severe-incident final due is one month from the 72-hour submission.

HOW TO USE THE EXAMPLES

1. Compare the example to your facts, but create a new operational Event ID in Event Intake.
2. After prompt initial assessment, record the earliest reasonable-certainty awareness time and factual basis. Do not backfill it to when the investigation or internal approval finished.
3. Use Trigger Assessment as an escalation aid, not as an automated legal conclusion.
4. Populate Notification Data once; the three packet tabs then assemble the stage-specific internal preparation views.
5. Submit only through the live ENISA SRP and preserve the platform confirmation in Submission Log.

ILLUSTRATIVE ONLY

AEV scenario

Fictional SmartGate Controller v4.2 progresses from customer signal to staged reporting and corrective-measure evidence.

Severe incident

Fictional FleetCloud Update Service tracks a compromised update channel, containment, submission, and final-report controls.

Deadline sequence

Illustrative first-signal, reasonable-certainty awareness, 24-hour, 72-hour, and final milestones show how stage records connect.

Evidence references

Synthetic IDs demonstrate linkage without exposing confidential or production records.

Do not copy conclusions

Each real event still requires fact-specific technical and legal review.

Map the internal record to ENISA reporting stages

The SRP Field Map is based on ENISA's published FAQ updated August 31, 2026 and is designed to be re-checked against the live platform before production use.

	A	B	C	D	E	F	G	H
1	**ENISA Single Reporting Platform Field Map**							
2	*Field-stage matrix based on ENISA's SRP FAQ updated 31 August 2026. Re-check the official source before each production use.*							
3								
4	*LEGEND: X = obligatory | C = copied from prior stage or updated | O = optional | I = obligatory if available | A = automated / not visible to submitter*							
5								
6	**Field ID**	**Section**	**SRP Field**	**24h**	**72h**	**Final**	**Operational Note**	**Official Source**
7	1	Common	Notification type (Vulnerability / Incident)	X	C	C	Select the event type and keep it consistent across stages.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
8	2	Common	Notification level (24h / 72h / Final)	X	X	X	Stage is selected or generated for each submission.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
9	3	Common	Reporting time - 24h	A	A	A	Platform-generated timestamp.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
10	4	Common	Reporting time - 72h	A	A	A	Platform-generated timestamp.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
11	5	Common	Reporting time - Final	A	A	A	Platform-generated timestamp.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
12	6	Common	Reporter	A	A	A	Derived from the SRP Assigned Representative (platform-user) account; this role is distinct from a CRA Article 18 authorised representative.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
13	7	Common	Name of manufacturer or open-source software steward	X	C	C	Verify legal reporting entity.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
14	8	Common	Product	X	C	C	Use a controlled product name and version reference.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
15	9	Common	Product Type (Default / Important / Critical)	O	C	C	Determine under current CRA rules; do not guess.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
16	10	Common	Product Category (Annex III / IV where applicable)	O	C	C	Complete when Product Type is not Default.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
17	11	Common	Member States where product is available	I	C	C	Obligatory at 24h if information is available.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
18	12	Common	Title	X	C	C	Use a concise internal title that can remain stable.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
19	v13	Vulnerability	CVE ID	O	C	C	Enter when assigned or known.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions
20	v14	Vulnerability	EUVD ID	O	C	C	Enter when assigned or known.	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions

Stage legend

X required | C copied or updated | O optional | I required if available | A platform-generated or not visible to submitter

Move from first signal to an evidence-backed record

The full package gives your team editable controls for the 24-hour, 72-hour, and final-report workflow - with implementation guidance for the first critical hours.

THE COMPLETE EARLY-ACCESS PACKAGE

- 20-tab Excel readiness and evidence system
- 24/72-Hour Reporting Quick Guide - PDF and editable DOCX
- First Four Hours Runbook - PDF and editable DOCX
- Early-access README with implementation and update terms
- One no-cost v1.1 alignment update after live SRP verification

WHAT THIS PREVIEW INTENTIONALLY OMITS

- ☑ Editable workbook and downloadable source files
- ☑ Formula logic, validation rules, and most workbook rows
- ☑ Full stage packets, checklists, reference tables, and exercises
- ☑ Any real customer, employee, incident, or product data

Get the full system - $149
SECURE CHECKOUT ON PAYHIP

See product details
syntera systems.com

Product edition current through September 3, 2026
Includes ENISA SRP FAQ updates published August 31, 2026.

Scope: operational reporting-readiness and evidence control only. The system does not determine legal applicability or reportability, provide legal advice, perform incident response or cybersecurity engineering, submit notifications, replace the ENISA platform, or certify CRA compliance.

Official references: CRA Regulation (EU) 2024/2847 | ENISA Single Reporting Platform FAQ