

EU Digital Compliance Practical Guideline

Actions and evidence for nine EU digital laws

SCAI – Swiss Cyber AI | 8 October 2026 | www.swisscyberai.org

A working guide for security, IT, legal, privacy, procurement and business teams. Confirm scope, assign owners, close urgent gaps, test the controls and keep evidence.

Use this guide in three working sessions

Session	Do the work	Leave with
1 Scope 60 minutes	Legal and business owners review the law table and scope questions on pages 2 and 3.	A signed scope record for each entity or service.
2 Assign 90 minutes	Owners use pages 4 to 16 and supplier checks on page 20 to identify gaps.	Named actions, due dates and evidence requirements.
3 Prove Half a day	Exercise incident reporting, restore a service and sample evidence. Use pages 17 to 23.	Test results and a funded 90-day plan.

Find what you need

Pages	Working material
2 to 6	Linked EU law table, applicability, ownership and shared controls
7 to 16	NIS2 and practical checklists for all nine laws
17 to 19	Incident response and reporting clocks
20 to 23	Supplier review, 90-day plan and reusable records
24	Dates to track and supplementary official sources

How to read the actions: Pink underlined citations open the named article or paragraph on EUR-Lex. Lettered points are identified in the label. “Supports” links an implementation recommendation to its legal purpose; it does not make that method or target mandatory. Quotations are short verbatim excerpts; read the full provision for conditions.

Apply each duty only within its scope, role and effective date. Add national implementing and sector rules. Owners, tests and the 90-day plan are recommendations; this guide does not certify compliance.

EU laws and official links

Click the legal instrument in the last column. On EUR-Lex, check the current consolidated version, amendments and applicable implementing acts. The next pages explain how to act on each instrument.

Law	When to assess it	First output	Official EU text
GDPR	Processing personal data within Article 3 territorial scope.	Processing and data-flow register.	Regulation 2016/679 Arts 3, 5, 24, 28, 30 to 35
NIS2	Covered sector or service, size rules and exceptions. National law determines local implementation.	Entity classification and local reporting route.	Directive 2022/2555 Arts 2 to 4, 20, 21, 23, 26
DORA	Listed financial entities. Separate rules govern designated critical ICT providers.	ICT framework and supplier register.	Regulation 2022/2554 Arts 2, 5 to 16, 19, 24 to 30
AI Act	Providing or deploying AI within the Act's scope. Role and intended purpose determine duties.	AI inventory and classification.	Regulation 2024/1689 Arts 2 to 6, 16, 26, 50, 53, 113
CRA	Relevant hardware or software products made available on the EU market.	Product scope and vulnerability reporting process.	Regulation 2024/2847 Arts 2, 13, 14, 32, 69, 71; Annex I
CER	Entities identified as critical under national implementation.	Designation record and all-hazards risk plan.	Directive 2022/2557 Arts 6, 8, 12 to 15
Data Act	Connected product data, related services, data sharing or data processing services.	Data-access process and tested cloud exit.	Regulation 2023/2854 Arts 1 to 5, 13, 23 to 31, 50
eIDAS	Electronic identity, signatures, seals and trust services; duties depend on role.	Signing policy and trust-service validation.	Regulation 910/2014 As amended by 2024/1183
DSA	Intermediary services offered to EU recipients; layers depend on service type and size.	Service classification and notice process.	Regulation 2022/2065 Arts 2, 11 to 18, 19 to 32, 33

AI Act: read with Regulation (EU) 2026/1744, which changes parts of the timetable and obligations. eIDAS: the linked consolidation includes the European Digital Identity amendment. NIS2 and CER need a national-law entry as well as the EU link.

Legal anchors [AI Act amendment 2026/1744](#) | [eIDAS amendment 2024/1183](#)

Decide what applies

Complete one scope record per legal entity and relevant activity. A group-level label is not enough. A Swiss headquarters does not settle the position of EU subsidiaries, EU-market products or services offered into the EU.

Ask in this order	What to record	Route
1 Which entity and activity?	Legal name, country, establishment, service, product, customers and EU connection. NIS2 Art 26 · GDPR Art 3 · DSA Art 2(1)	Open a record on page 22.
2 Are people's data processed?	Controller or processor role, people affected and Article 3 territorial analysis. GDPR Art 3 · GDPR Art 4(7) · GDPR Art 4(8)	GDPR on page 9.
3 Is the entity in a covered sector?	Actual services, NIS2 Annex I or II category, EU size calculation, exceptions and national law. NIS2 Art 2 · NIS2 Annex I · NIS2 Annex II	NIS2 on pages 7 and 8.
4 Is it a regulated financial entity?	Exact Article 2 category, exclusions and simplified regime if relevant. DORA Art 2 · DORA Art 16	DORA on page 10.
5 Is AI provided or used?	Intended purpose, provider/deployer role, prohibited/high-risk/transparency/GPAI analysis. AI Act Art 2 · AI Act Art 5 · AI Act Art 6	AI Act on page 11.
6 Are digital products sold?	Manufacturer/importer/distributor role, product boundary, exclusions and EU-market placement. CRA Art 2 · CRA Art 3 · CRA Art 32	CRA on page 12.
7 Is there a critical-entity notice?	Designation, receipt date, covered service and sector-specific exclusions. CER Art 6(3) · CER Art 8	CER on page 13.
8 What data or online services exist?	Connected products, cloud services, trust services, user hosting or marketplace functions. Data Act Art 1 · eIDAS Art 2 · DSA Art 3(g)	Pages 14 to 16.

Approve a conclusion that can be checked

Use one of four outcomes: applies now; applies from a stated date; does not apply with reasons; unresolved with a named reviewer and due date. Attach the facts and legal provision supporting the conclusion.

Treat a supplier contract as a separate source of obligations. Selling to a regulated customer may create contract requirements even where the supplier is outside that law's direct scope. DORA's relationship with NIS2 must be assessed for the covered financial entity and relevant requirements.

Reopen scope when something changes

- New country, acquisition, service, product, AI purpose, customer segment or regulator notice.
- A significant change in size, outsourcing, branding, product modification or legal text.

Legal anchors [NIS2 Arts 2 to 4](#) | [GDPR Art 3](#) | [DORA Arts 1 and 2](#)

Assign ownership and define completion

Management remains accountable for the duties allocated to it by law. The CISO coordinates security work; business, privacy, legal and product owners must own their parts. Substitute actual names for the roles below.

Role	Practical responsibility	Evidence of completion
Executive sponsor	Approve scope, priorities, resources and material risk decisions. Resolve overdue critical actions. Supports: NIS2 Art 20(1) · DORA Art 5(2)	Dated decisions, budget and follow-up.
Legal or compliance	Confirm legal roles, national rules, authority routes and deadlines; maintain the legal register. Supports: NIS2 Art 2 · NIS2 Art 23 · GDPR Art 24(1)	Reviewed scope and reporting records.
CISO and security operations	Coordinate cyber controls, detection, response and assurance. Record coverage gaps. Supports: NIS2 Art 21(1) · DORA Art 5(2)(c)	Control owners, test results and incident records.
CIO and service owners	Maintain assets, access, configuration, remediation and service restoration. Supports: DORA Art 8(1) · DORA Art 9(4) · DORA Art 12(1)	Coverage exports and recovery results.
Privacy lead and DPO	Privacy lead operates the programme; the DPO, where appointed, advises and monitors independently. Supports: GDPR Art 24(1) · GDPR Art 38 · GDPR Art 39(1)	Processing records, advice and rights cases.
Product or AI owner	Own product lifecycle or AI intended use, release decisions, monitoring and support. Supports: CRA Art 13 · AI Act Art 16 · AI Act Art 26	Classification, release approval and change history.
Procurement and supplier owner	Perform due diligence; obtain terms, monitor suppliers and maintain exit plans. Supports: NIS2 Art 21(2)(d) · DORA Art 28	Approved supplier record and tested exit.
Assurance reviewer	Sample evidence independently of the control operator where practical; verify closure. Supports: NIS2 Art 21(2)(f) · DORA Art 6(6)	Findings, retests and closure decisions.

Use a strict definition of done

- The control has a defined scope, named owner and documented operating method.
- Implementation covers the intended population; exclusions are visible and approved.
- A dated test demonstrates the required result; failures have an action and deadline.
- The evidence link works and shows the relevant entity, system, period and reviewer.

Run a short monthly review

Review new scope, overdue high-risk actions, failed tests and reporting readiness. Ask management for a specific decision when a gap needs funding or risk acceptance. Review the complete programme at least quarterly as a suggested operating cadence.

Legal anchors [NIS2 Art 20](#) | [DORA Art 5](#) | [GDPR Arts 24 and 38](#)

Implement the common security baseline

Use existing NIST or other controls where they fit. The following are practical starting controls, not an EU certification checklist. Set risk-based frequencies and targets, then apply stricter law or contract requirements where relevant.

Control and action	Suggested owner	Proof to sample
01 Inventory critical services, IT, cloud, OT, data and dependencies. Reconcile discovery against the register. Supports: NIS2 Art 21(2)(i) · DORA Art 8(1)	Service owners	Unmanaged-asset exceptions and dependency map.
02 Enforce strong authentication and least privilege. Separate administrator accounts; control emergency access. Supports: NIS2 Art 21(2)(i)-(j) · DORA Art 9(4)(c)-(d)	Identity team	Test sign-in, privileged review and leaver removal.
03 Prioritise vulnerabilities by exploitation, exposure and service impact. Give exceptions an expiry. Supports: NIS2 Art 21(2)(e) · DORA Art 9(4)(f)	IT and OT	Sample an urgent finding through remediation and retest.
04 Apply secure configuration and endpoint protection. Include servers and unsupported devices in gap reporting. Supports: DORA Art 9(2)-(3) · NIS2 Art 21(1)	IT operations	Coverage report and a tested detection response.
05 Segment critical systems and protect remote access. Test supplier access and emergency isolation. Supports: DORA Art 9(4)(b) · NIS2 Art 21(1)	Network and OT	Allowed-path test and authorised isolation exercise.
06 Collect useful security logs, monitor alerts and maintain an out-of-hours response route. Supports: DORA Art 10(1)-(3) · NIS2 Art 21(2)(b)	Security operations	Detection-to-response record; escalation answered.
07 Protect backups from production compromise. Restore a complete business service. Supports: NIS2 Art 21(2)(c) · DORA Art 12(1)-(3)	Service owners	Actual restore time, data integrity and business sign-off.
08 Assess critical suppliers, concentration and subcontractors; agree rapid incident assistance. Supports: NIS2 Art 21(2)(d) · DORA Art 28(4) · DORA Art 30	Procurement	Risk assessment, contract and tested contact route.
09 Protect sensitive data with access rules, encryption and controlled retention. Supports: GDPR Art 5(1)(e)-(f) · GDPR Art 32(1)(a) · NIS2 Art 21(2)(h)	Data owners	Access sample, key recovery and deletion evidence.
10 Train relevant staff and management; exercise incidents, continuity and legal reporting. Supports: NIS2 Art 20(2) · NIS2 Art 21(2)(g) · DORA Art 13(6)	HR and CISO	Role-specific training and exercise actions closed.

Prioritise without waiting for the complete programme

Escalate exposed privileged access, exploited weaknesses, missing critical backups and an unusable reporting route immediately. Assign a temporary safeguard and a permanent fix. An approved plan alone does not reduce the exposure.

Legal anchors [NIS2 Art 21](#) | [GDPR Art 32](#) | [DORA Arts 6 to 14](#)

Connect controls to duties and decisions

Keep one evidence set where work is shared, while retaining the specific legal requirement and remaining gap. A maturity score or certification is supporting evidence within its scope; it is not automatic compliance with these laws.

Shared work	Legal anchors it can support	Keep the difference visible
Risk assessment	NIS2 Art 21(2)(a) · DORA Art 6(1) · GDPR Art 35(1) · CER Art 12 · AI Act Art 9	Service risk, harm to people, physical resilience and AI risk have different tests.
Access and recovery	GDPR Art 32(1)(b)-(c) · NIS2 Art 21(2)(c) · DORA Art 9 · DORA Art 12	Check system population, business recovery and the evidence period.
Secure development	CRA Art 13(1)-(2) · CRA Annex I · NIS2 Art 21(2)(e) · AI Act Art 9	Product conformity and AI role duties need separate assessment.
Supplier review	GDPR Art 28(3) · NIS2 Art 21(2)(d) · DORA Art 28 · DORA Art 30 · Data Act Art 25	Processing terms, financial ICT terms and switching rights differ.
Incident handling	GDPR Art 33 · GDPR Art 34 · NIS2 Art 23 · DORA Art 19 · CRA Art 14 · CER Art 15	Trigger, obligated entity, authority, clock and report content differ.

Make each risk decision executable

Record the scenario, affected service and people, existing safeguards, plausible impact and treatment. Select an owner and due date. Define the test that will show the risk has reduced. Escalate a risk the owner cannot fund or lawfully accept.

Use exceptions with an expiry date

An exception needs the affected scope, reason, compensating control, approving authority, expiry and closure test. Risk acceptance cannot waive a legal duty. Legal must assess whether the proposed temporary arrangement is permissible.

Example of an honest mapping

A restore test demonstrates recovery of application A within its agreed objective. Link it to the relevant availability and restoration duties. Keep the missing supplier dependency or untested identity service as an open gap. Do not label the whole law complete.

Change gate

Before a new service, supplier, AI use or product release: repeat scope, update risk, confirm required notices or conformity steps, test controls and record the business approval. Repeat when the intended use changes.

Legal anchors [NIS2 Art 21](#) | [GDPR Arts 25 and 35](#) | [CRA Annex I](#)

NIS2 scope and management

Decide coverage at legal-entity and service level. Use the applicable national implementing law; do not wait for a regulator letter where the law requires self-assessment or registration.

From the law “approve the cybersecurity risk-management measures” [NIS2 Art 20\(1\)](#)

Management approval is explicit in the EU text; implement it through the national law.

Step	Action	Required output
1 Match the activity	Map actual services to Annex I or II and national categories. Relevant areas include energy, transport, health, water, digital infrastructure, ICT service management and specified manufacturing. NIS2 Art 2(1) · NIS2 Annex I · NIS2 Annex II	Sector and service rationale with exact provision.
2 Calculate size	Apply the EU enterprise-size rules, including relevant partner and linked enterprises. Record employees and financial data. Check exceptions covering certain smaller entities. NIS2 Art 2(1)-(2)	Calculation and exception analysis reviewed by Legal.
3 Classify the entity	Determine essential or important status under Article 3 and national rules. Check special designations and cross-border jurisdiction. NIS2 Art 3(1)-(2) · NIS2 Art 26	Entity classification and competent authority.
4 Register as required	Confirm local deadlines, registration data, portal access and change notifications. Record an owner and deputy. NIS2 Art 3(4) · NIS2 Art 27(2)-(3)	Submission receipt or documented reason registration is not required.
5 Obtain management action	Management approves and oversees the required risk measures and undertakes the required training. Record decisions and resources. NIS2 Art 20(1)-(2)	Minutes, training evidence and action owners.
6 Prepare reporting	Set significance criteria and reporting clocks. Certain digital providers fall under Regulation 2024/2690. NIS2 Art 23(3)-(4) · 2024/2690 Art 3	Local procedure, tested channel and incident drill.

Practical classification questions

- Do we operate a covered service ourselves, or only buy it from a provider?
- Does manufacturing activity match a listed category rather than manufacturing in general?
- Does a small-entity exception, critical-entity designation or sector-specific law change the result?

Overlap check: For financial entities covered by DORA, review the sector-specific relationship under NIS2 Article 4. Keep GDPR and any product or other obligations in the assessment.

Legal anchors [NIS2 Arts 2 to 4 and 20](#) | [Digital-sector implementing rules](#)

NIS2 implementation checklist

Article 21 requires proportionate technical, operational and organisational measures. Use all ten areas below as a completeness check, with national requirements and risk assessments determining the precise implementation.

From the law “policies and procedures to assess the effectiveness of cybersecurity risk-management measures” [NIS2 Art 21\(2\)\(f\)](#)

Keep test results and corrective actions, not only policies.

Article 21 area	Practical action	Evidence
Risk analysis and security policy	Approve a service-based risk assessment and a usable security policy. NIS2 Art 21(2)(a)	Current assessment, approval and treatment plan.
Incident handling	Define triage, response authority, containment and reporting decisions. NIS2 Art 21(2)(b)	Runbook, exercise and case record.
Continuity and crisis management	Set service recovery objectives; protect backups and test restoration. NIS2 Art 21(2)(c)	Recovery results and crisis exercise.
Supply-chain security	Assess direct suppliers and service providers; address relevant vulnerabilities and secure practices. NIS2 Art 21(2)(d)	Supplier register, decisions and contracts.
Acquisition and development	Include security in design, changes, maintenance and vulnerability handling or disclosure. NIS2 Art 21(2)(e)	Release evidence and vulnerability queue.
Effectiveness assessment	Test whether controls operate across their claimed scope. NIS2 Art 21(2)(f)	Sample results, failures and retests.
Cyber hygiene and training	Train users and management for their roles and current risks. NIS2 Art 21(2)(g)	Training record and learning checks.
Cryptography	Define where and how to use encryption; manage keys and recovery. NIS2 Art 21(2)(h)	Standard, key ownership and tested recovery.
People access and assets	Manage joiners, movers, leavers, privileged rights and asset ownership. NIS2 Art 21(2)(i)	Access review and asset reconciliation.
Authentication and communication	Apply MFA or continuous authentication and secure communication where appropriate. NIS2 Art 21(2)(j)	Configuration, exceptions and emergency channel test.

Prove three things in the first month

- A leaver loses access, including privileged and third-party access, within the approved target.
- A critical service can be restored with its identity, network and supplier dependencies.
- The incident team can reach the correct authority route and prepare a timely early warning.

Regulation 2024/2690 provides detailed requirements for specified digital entities. Its checklist is not automatically binding on every NIS2 sector.

Legal anchors [NIS2 Art 21](#) | [Regulation 2024/2690](#)

GDPR practical checklist

Assess controllers and processors separately. Employee and business-contact data are personal data; B2B activity is not a blanket exemption. The controller owns accountability; the data protection officer (DPO) advises and monitors where appointed.

From the law “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1” [GDPR Art 5\(2\)](#)

Make the evidence for each control easy to retrieve.

Actions and evidence

Action	Suggested owner	Keep as evidence
Identify purposes, data, people, recipients and retention. Document lawful bases and special-category conditions where needed. GDPR Art 5(1) · GDPR Art 6 · GDPR Art 9 · GDPR Art 30	Business and privacy	Processing record, legal basis and data-flow map.
Provide clear notices; collect only necessary data. Define retention and an effective deletion process. GDPR Art 5(1)(c)-(e) · GDPR Art 13 · GDPR Art 14	Data owners	Published notices and a sample deletion result.
Put Article 28 terms in place with processors. Review subprocessors, international transfers and the relevant safeguards. GDPR Art 28(2)-(3) · GDPR Art 44 · GDPR Art 46	Legal and procurement	Processing terms and transfer assessment.
Implement risk-appropriate security. Screen processing for a data protection impact assessment (DPIA); complete it before high-risk processing. GDPR Art 32(1) · GDPR Art 35(1)	CISO and privacy	Control results, DPIA and treatment decisions.
Handle rights requests securely. Track the one-month response period and any lawful extension; explain it within the first month. GDPR Art 12(3) · GDPR Art 12(6) · GDPR Art 15	Privacy operations	Identity check, response and deadline record.
Prepare breach decisions and communications. Document every personal data breach, including decisions not to notify. GDPR Art 33(5) · GDPR Art 34	Incident lead and privacy	Breach log, risk assessment and receipts.

Suggested test and supporting provisions

- Trace one employee or customer record from collection to deletion, including supplier copies.
- Run a mock access request and a breach involving loss of availability as well as confidentiality.

Tests support: [GDPR Art 5\(2\)](#) · [GDPR Art 12\(3\)](#) · [GDPR Art 32\(1\)\(d\)](#)

Watch for: Consent is not the default basis for every activity. An encrypted dataset may still be personal data. Security incidents can be personal data breaches without confirmed exfiltration.

Legal anchors [GDPR Arts 5 to 6, 12, 28, 30 to 35](#)

DORA practical checklist

DORA has applied since 17 January 2025 to listed financial entities, subject to its exclusions and proportionality rules. Ordinary ICT suppliers face customer contracts; designated critical ICT third-party providers have a separate oversight regime.

From the law “define, approve, oversee and be responsible for the implementation” [DORA Art 5\(2\)](#)
Record management decisions and follow-up on the ICT framework.

Actions and evidence

Action	Suggested owner	Keep as evidence
Map critical or important functions to systems, data, people and suppliers. Identify concentration and single points of failure. DORA Art 8(1) · DORA Art 8(5) · DORA Art 29(1)	Business and IT	Function map and dependency assessment.
Maintain the management-approved ICT risk framework, continuity, recovery and communication arrangements. DORA Art 5(2) · DORA Art 6(1) · DORA Art 11 · DORA Art 14	Management and risk	Approved framework, review and treatment records.
Classify incidents using applicable criteria and prepare major-incident reports. Record awareness and classification separately. DORA Art 18(1) · DORA Art 19(1) · 2025/301 Art 5	Incident lead	Classification checklist and reporting chronology.
Run a proportionate resilience-testing programme. Determine whether advanced threat-led penetration testing applies. DORA Art 24(1)-(2) · DORA Art 26	CISO and risk	Test plan, findings, retests and TLPT decision.
Maintain the prescribed register of ICT contractual arrangements. Address due diligence, concentration, subcontracting and mandatory terms. DORA Art 28(3)-(4) · DORA Art 29 · DORA Art 30	Procurement and Legal	Register, contracts and provider assessments.
Test continuity and exit for important dependencies. Confirm usable exports, replacement skills, capacity and realistic timings. DORA Art 11(6) · DORA Art 28(8)	Service owners	Restore or exit rehearsal and business acceptance.

Suggested test and supporting provisions

- Simulate loss of the identity service used by both production and disaster recovery.
- Prepare a major-incident notification within the relevant four-hour and 24-hour limits on page 18.

Tests support: [DORA Art 11\(6\)](#) · [DORA Art 24\(1\)](#) · [2025/301 Art 5](#)

Watch for: Outsourcing reporting or operations does not transfer the financial entity's responsibility. A generic vendor list does not replace the prescribed register of information.

Legal anchors [DORA Arts 5 to 16, 19, 24 to 30](#) | [Reporting time limits](#)

AI Act practical checklist

Classify the actual system and intended use. Record whether the entity provides, deploys, imports or distributes it, and distinguish the application from its general-purpose AI (GPAI) model. Reassess when the use or system changes.

From the law “take measures to support the development of AI literacy” [AI Act amended Art 4\(1\)](#)

This is the amended Article 4(1); tailor literacy measures to the actual uses and risks.

Actions and evidence

Action	Suggested owner	Keep as evidence
Inventory AI uses, owners, inputs, outputs, affected people, connected tools and suppliers. Screen for prohibited practices before use. AI Act Art 2(1) · AI Act Art 3(3)-(4) · AI Act Art 5 · AI Act amended Art 5(1a)	Business and Legal	AI register, purpose and prohibition check.
Assess high-risk, transparency and GPAI duties. Record role, legal rationale and effective date; review changes or rebranding. AI Act Art 6 · AI Act Art 25(1) · AI Act Art 50 · AI Act Art 53 · 2026/1744 Art 1(40)	AI governance	Signed classification and change triggers.
Apply current disclosure and literacy duties. Train people for actual uses and risks; give required interaction or content notices. AI Act amended Art 4(1) · AI Act Art 50(1)-(4)	Business and HR	Notices, training materials and attendance.
For relevant high-risk duties, plan provider documentation, quality controls and conformity, or deployer oversight and monitoring. AI Act Art 16 · AI Act Art 17 · AI Act Art 26 · AI Act Art 43 · 2026/1744 Art 1(40)	Product or business	Role-specific requirement and evidence list.
Assess personal data and harmful outcomes. Test representative cases, limitations and meaningful human intervention. GDPR Art 35(1) · AI Act Art 9 · AI Act Art 14 · AI Act Art 27(1)	Privacy and business	DPIA where required, tests and release decision.
For agents, restrict tool permissions and data access; set action limits, approval points and a tested shutdown route. Supports: AI Act Art 14(4)(d)-(e) · AI Act Art 15(5) · GDPR Art 32(1)	Engineering and CISO	Permission map, action logs and stop test.

Suggested test and supporting provisions

- Ask an owner to explain the intended purpose, legal role and why the system is permitted.
- Test one incorrect output and one unauthorised tool instruction; verify intervention and recovery.

Tests support: [AI Act Art 14](#) · [AI Act Art 15](#) · [2026/1744 Art 1\(40\)](#)

Watch for: Agent controls in the last row are practical recommendations, not a mandated architecture. The 2026 amendment changes high-risk dates; see page 24. Other applicable duties continue.

Legal anchors [AI Act](#) | [2026 amendment](#)

Cyber Resilience Act practical checklist

Determine whether the product with digital elements is in scope and which economic-operator role applies. Article 14 reporting has applied since 11 September 2026; most requirements apply from 11 December 2027.

From the law “be made available on the market with a secure by default configuration” [CRA Annex I Part I \(2\)\(b\)](#)

Apply the risk and applicability conditions and the tailored B2B exception in the full provision.

Actions and evidence

Action	Suggested owner	Keep as evidence
Define product boundaries, essential remote processing, versions, EU-market placement and exclusions. Classify the conformity route. CRA Art 2 · CRA Art 3(1)-(2) · CRA Art 32	Product and Legal	Scope, role and conformity decision.
Perform a product cybersecurity risk assessment. Build security requirements into design, defaults, access and updates. CRA Art 13(1)-(3) · CRA Annex I Part I	Engineering	Threat assessment, requirements and security tests.
Track software components and vulnerabilities. Prepare the machine-readable software bill of materials and a disclosure channel. CRA Annex I Part II (1), (5)-(6)	Product security	Component inventory, SBOM and intake records.
Fund lifecycle support and secure updates. Set a justified support period; generally at least five years unless expected use is shorter. CRA Art 13(8) · CRA Art 13(19) · CRA Annex I Part II (7)-(8)	Product management	Support decision, published end date and update tests.
Prepare technical documentation, required instructions, EU declaration and CE marking through the applicable conformity process. CRA Art 13(12) · CRA Art 28 · CRA Art 30 · CRA Art 31 · CRA Art 32	Product and quality	Release file and conformity evidence.
Operate reporting now for qualifying exploited vulnerabilities and severe incidents. Include eligible legacy products under Article 69. CRA Art 14(1)-(4) · CRA Art 69(3) · CRA Art 71	Product response team	24-hour contact route, classification and submissions.

Suggested test and supporting provisions

- Select a released product: identify affected versions, components, support owner and customer contact route.
- Run a vulnerability scenario through assessment, reporting, fix distribution and user instructions.

Tests support: [CRA Art 13\(2\)](#) · [CRA Art 14](#) · [CRA Annex I Part II](#)

Watch for: Standalone SaaS is not automatically a CRA product. Necessary remote processing can form part of a product. Product support must reflect expected use; five years is not always sufficient.

Legal anchors [CRA Arts 13, 14, 32, 69 and 71](#)

Critical Entities Resilience practical checklist

CER addresses the resilience of designated critical entities and essential services against physical and other disruption. Confirm the national designation and notice. Sector-specific exclusions matter, including for banking, financial market infrastructure and digital infrastructure.

From the law *“appropriate and proportionate technical, security and organisational measures to ensure their resilience”*
[CER Art 13\(1\)](#)

Link measures to the entity risk assessment and national implementation.

Actions and evidence

Action	Suggested owner	Keep as evidence
Record the designation notice, receipt date, service, authority and obligations. Confirm sector and national exceptions. CER Art 6(3) · CER Art 8	Legal and continuity	Designation file and applicable deadlines.
Assess natural and human-caused hazards, including power, water, access, people, sabotage and cross-border dependencies. CER Art 12(1)-(2)	Continuity and facilities	All-hazards risk assessment.
Protect sites and operations proportionately. Define access, physical safeguards and personnel measures permitted by law. CER Art 13(1)(a)-(b), (e) · CER Art 14	Facilities and HR	Controls, authorised access and lawful checks.
Plan continuity, workarounds and recovery. Confirm resource needs, alternatives and minimum viable service levels. CER Art 13(1)(c)-(d)	Business owner	Resilience plan and dependency arrangements.
Train staff and exercise disruption. Assign a liaison and prepare significant-incident reporting. CER Art 13(1)(f) · CER Art 13(3) · CER Art 15(1)	Continuity lead	Exercise, contact card and notification process.
Track the notification-based timetable. Risk assessment is due within nine months; Chapter III generally applies after ten months. CER Art 6(3) · CER Art 12(1)	Legal and sponsor	Dated plan linked to the actual notice.

Suggested test and supporting provisions

- Exercise a prolonged power or water loss with loss of site access and one unavailable key supplier.
- Demonstrate the minimum service that can continue, for how long, with which people and resources.

Tests support: [CER Art 13\(1\)\(c\)-\(d\), \(f\)](#)

Watch for: A cybersecurity recovery plan alone does not cover physical resilience. NIS2 and CER classifications and local obligations need separate records even where evidence is shared.

Legal anchors [CER Arts 6, 8 and 12 to 15](#)

Data Act practical checklist

Map each role: connected-product manufacturer, related-service provider, user, data holder, data recipient or data-processing-service provider. A cloud customer should also use the switching rules in procurement and exit planning.

From the law “Providers of data processing services shall take the measures provided for in Articles 25, 26, 27, 29 and 30” [Data Act Art 23](#)

Read the full switching duty, including its role, scope and exceptions.

Actions and evidence

Action	Suggested owner	Keep as evidence
Identify product and related-service data, metadata, access routes and the party holding each dataset. Data Act Art 2(15)-(17) · Data Act Art 3(1)	Product and data owner	Data catalogue and role map.
Provide required pre-contract information and applicable user access. Verify identity and authority without obstructive procedures. Data Act Art 3(2)-(3) · Data Act Art 4(1)	Product and operations	Disclosures, request route and delivered sample.
Handle eligible third-party sharing. Check GDPR, trade secrets, permitted uses and necessary protective measures. Data Act Art 4(6)-(9) · Data Act Art 5 · Data Act Art 6	Legal and privacy	Sharing decision, safeguards and access terms.
Review relevant data terms for unfair clauses and transparency. Assess mandatory public-body requests through Legal. Data Act Art 13 · Data Act Art 14 · Data Act Art 17	Legal and procurement	Contract review and request assessment.
For cloud or other covered processing services, define exportable data, interfaces, transition, assistance, charges and deletion. Data Act Art 25 · Data Act Art 27 · Data Act Art 29 · Data Act Art 30	Service owner	Contract and executable switching plan.
Test an export into an alternative environment; reconcile records and record feature or interoperability limits. Supports: Data Act Art 23(c)-(d) · Data Act Art 30	IT and business	Export/import test and exit action list.

Suggested test and supporting provisions

- Request a representative connected-product dataset and check completeness, format, metadata and authorisation.
- Read exported cloud data with an independent tool and measure the actual time and effort.

Tests support: [Data Act Art 4\(1\)](#) · [Data Act Art 23\(c\)](#) · [Data Act Art 30](#)

Watch for: The Data Act is not a general right to all company data and does not override GDPR. Switching-charge removal does not mean every service fee or early-termination charge disappears.

Legal anchors [Data Act Arts 3 to 5, 13, 23 to 31 and 50](#)

eIDAS and digital trust practical checklist

Separate a business using electronic signatures or identity from a provider of regulated trust services. The operational checklist below starts with the relying business; providers and wallet participants need additional role-specific requirements.

From the law *“A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.”* [eIDAS Art 25\(2\)](#)

Check signing authority and national transaction formalities separately.

Actions and evidence

Action	Suggested owner	Keep as evidence
List transactions, countries, parties and formal requirements. Decide the necessary signature or seal level for each process. Supports: eIDAS Art 2(3) · eIDAS Art 25 · eIDAS Art 35	Legal and process owner	Transaction-to-signature policy.
Select and verify the service. Where qualified status is required, check the specific service on the official trusted lists. eIDAS Art 22(1) · eIDAS Art 32(1)	Procurement and Legal	Dated service-status validation.
Check identity and authority to sign. Protect signing credentials and define delegation, revocation and leaver handling. Supports: eIDAS Art 26 · eIDAS Art 32(1)	Identity and business	Identity record and signing authority.
Preserve the signed file, validation result, certificates, time information and evidence needed for later verification. Supports: eIDAS Art 32(1) · eIDAS Art 34	Records owner	Validation and retention package.
Test validation beyond the live vendor portal. Define how long-term evidence survives contract end or provider failure. Supports: eIDAS Art 32 · eIDAS Art 34	IT and records	Independent validation and export test.
If offering identity or trust services, assess conformity, supervision, incidents and EUDI wallet duties separately. eIDAS Art 5a · eIDAS Art 19a · eIDAS Art 20 · eIDAS Art 24	Service owner and Legal	Role-specific compliance and reporting plan.

Suggested test and supporting provisions

- Verify a signed document without relying solely on a screenshot or vendor approval email.
- Check that the signatory was authorised for the transaction at the time of signing.

Tests support: [eIDAS Art 32](#) · [eIDAS Art 34](#)

Watch for: A qualified electronic signature has the EU legal effect of a handwritten signature, but it does not itself prove corporate signing authority or satisfy every national formality. An electronic seal is a different instrument.

Legal anchors [eIDAS Arts 22, 25, 32 and 35](#) | [EU trusted lists](#)

Digital Services Act practical checklist

Classify each service: mere conduit, caching, hosting, online platform, consumer marketplace or designated very large service. A corporate website publishing its own material is not automatically an online platform under the DSA.

From the law *“Those mechanisms shall be easy to access and user-friendly”* [DSA Art 16\(1\)](#)

Test the hosting notice mechanism with a realistic user submission.

Actions and evidence

Action	Suggested owner	Keep as evidence
Document the service functions, EU recipients and operator. Check the exact scope of size-related exemptions. DSA Art 2(1) · DSA Art 3(g), (i) · DSA Art 19(1) · DSA Art 29	Product and Legal	Service classification and exemption analysis.
Publish required contact information and terms. Explain content restrictions and relevant moderation policies clearly. DSA Art 11(1) · DSA Art 12(1) · DSA Art 14(1)	Legal and operations	Contact points, terms and publication record.
For hosting, implement usable illegal-content notices. Assess cases diligently, record decisions and issue required reasons. DSA Art 16(1)-(6) · DSA Art 17(1)-(3)	Trust and safety	Notice, assessment, decision and communication.
For applicable platforms, operate complaint handling and assess advertising, interface and minors-protection duties. DSA Art 20(1) · DSA Art 25 · DSA Art 26 · DSA Art 28	Product and operations	Complaint results and design checks.
For covered consumer marketplaces, implement trader traceability and applicable compliance-by-design measures. DSA Art 30(1)-(3) · DSA Art 31	Marketplace owner	Trader checks and listing workflow tests.
Track recipient numbers and any designation. If designated very large, implement the additional systemic-risk and audit regime. DSA Art 24(2) · DSA Art 33 · DSA Art 34 · DSA Art 37	Compliance	User calculation, designation and assurance plan.

Suggested test and supporting provisions

- Submit a realistic illegal-content notice and follow it through to a reasoned decision.
- Test an applicable user complaint, and check that operations can correct an earlier error.

Tests support: [DSA Art 16\(6\)](#) · [DSA Art 20\(4\)](#)

Watch for: Micro and small enterprise exemptions remove some duties, not the entire Act. Article 18 covers certain suspected criminal offences threatening life or safety; the DSA has no universal 72-hour cyber reporting rule.

Legal anchors [DSA Arts 11 to 18, 19 to 32 and 33 to 42](#)

Run the first hour of an incident

Start containment and legal triage together. The times below are suggested internal response targets, not statutory reporting periods. Do not delay a legally required report until root cause is confirmed.

Target	Action	Output
0 to 15 minutes	Appoint an incident lead and recorder. Protect safety, activate the contact route and preserve logs. Record discovery and known event times in UTC. Supports: NIS2 Art 21(2)(b) · DORA Art 17(3)(a)	Case ID, timeline and initial affected scope.
15 to 30 minutes	Contain under authorised procedures. For OT, involve the safety or plant owner before disruptive action where feasible. Identify affected entities, services, products and data. Supports: DORA Art 17(3)(b), (f) · NIS2 Art 21(2)(b)	Containment decisions and business impact.
By 30 minutes	Contact Legal, privacy, business and product owners as relevant. Assess each reporting trigger and record legal awareness or classification timestamps. Supports: GDPR Art 33(1) · NIS2 Art 23(3) · DORA Art 18(1)	Separate reporting decisions and deadlines.
By 60 minutes	Assign a submitter and deputy for each required route. Draft initial facts, unknowns and protective actions. Confirm customer and contractual notices. Supports: GDPR Art 33(3)-(4) · NIS2 Art 23(4) · DORA Art 19(1)	Approved first reports or a documented no-report decision.

Use one chronology and separate legal clocks

Record detection, awareness under each legal test, major/significant classification, each decision, submission and acknowledgement. The same event may trigger several laws for different group entities. One report does not automatically satisfy every regime.

Minimum incident record

- Case ID; legal entity; owner and deputy; affected services, countries, data and product versions.
- Confirmed facts; hypotheses; impact on operations and people; sources and timestamp of each update.
- Trigger assessment per law; exact deadline; recipient; approver; submitter; receipt; next update.
- Containment, recovery, evidence location and customer protection measures.

Before closing

Confirm all updates and final reports are complete. Record cause, service and data recovery, residual risk, actions, owners and retest dates. Keep the reasoning for decisions not to notify and reopen it when new facts emerge.

Legal anchors [GDPR Arts 33 and 34](#) | [NIS2 Art 23](#) | [DORA reporting rules](#)

Core incident reporting deadlines

Use these EU-level rules with the exact national route, thresholds, competent authority and applicable technical standards. All clocks are maximum limits; requirements to act without undue delay still apply.

Regime and trigger	First submission	Follow-up and recipient
GDPR controller Personal data breach unless unlikely to risk people's rights and freedoms.	Without undue delay; where feasible within 72 hours of awareness of the breach. Explain delay.	Competent data protection authority. Provide missing information in phases without undue further delay. Document all breaches. GDPR Art 33(1), (3)-(5)
GDPR processor and affected people	Processor: notify the controller without undue delay. Controller: communicate to people without undue delay when high risk, subject to Art 34 exceptions.	Do not give processors an assumed 72-hour allowance. Track contractual deadlines separately. GDPR Art 33(2) · GDPR Art 34(1)-(3)
NIS2 Significant incident under the applicable criteria.	Early warning within 24 hours of awareness of a significant incident; incident notification within 72 hours. Both without undue delay.	Competent CSIRT or authority. Final report within one month of the incident notification. Intermediate report if requested. NIS2 Art 23(3) · NIS2 Art 23(4)(a)-(d)
NIS2 ongoing incident and trust services	Trust service providers: the incident notification for qualifying trust-service incidents is within 24 hours, rather than 72.	If ongoing at the final-report date, provide progress then final report within one month after handling the incident. NIS2 Art 23(4)(b), (e)
DORA Major ICT-related incident under applicable classification rules.	As early as possible: within four hours of major classification and no later than 24 hours after awareness. If classified after 24 hours, within four hours of classification.	Competent financial authority. Intermediate within 72 hours of initial notification; update on recovery. Final within one month of intermediate or latest updated intermediate. DORA Art 19(1) · 2025/301 Art 5(1)-(4)

Set up the clocks before the exercise

For every entity, pre-fill the reporting portal, authority, relevant thresholds, local forms, submitter and deputy on page 22. Test access without sending a real incident notice.

DORA includes specific weekend and bank-holiday provisions and exceptions. Use continuous coverage as the operational default; rely on an extension only after confirming Article 5 eligibility and any authority decision.

Legal anchors [GDPR Arts 33 and 34](#) | [NIS2 Art 23](#) | [DORA Regulation 2025/301 Art 5](#)

Product and other reporting routes

Add these routes when the affected activity and legal role make them relevant. Confirm current effective dates and national implementation; do not apply a single generic notification deadline.

Regime and trigger	Clock and practical routing
CRA Actively exploited vulnerability	Manufacturer reports through the single platform to the coordinating CSIRT and ENISA. Early warning within 24 hours of awareness; vulnerability notification within 72 hours. Final report within 14 days after a corrective or mitigating measure becomes available. CRA Art 14(1)-(2)
CRA Severe incident affecting product security	Same recipients and platform. Early warning within 24 hours of awareness; incident notification within 72 hours. Final report within one month of the incident notification. Address affected-user information under Article 14. CRA Art 14(3)-(4), (8)
CER Significant or potentially significant disruption of essential services	Notify the competent authority without undue delay; initial notice within 24 hours of awareness unless operationally unable. Where relevant, provide a detailed report within one month; implement the national rule in the local runbook. CER Art 15(1)
AI Act Serious incident involving high-risk AI	Check role and transition first. Provider reports immediately on a causal link or reasonable likelihood, within 15 days of awareness. Widespread infringement or Art 3(49)(b) critical-infrastructure disruption: immediately, within two days. Death: immediately on a suspected link, within ten days. Route to the competent market-surveillance authority or AI Office under amended Art 75. AI Act Art 73(1)-(4) · AI Act Art 26(5) · AI Act amended Art 75(1a)
eIDAS Trust-service security breach or disruption	Non-qualified providers: Art 19a uses without undue delay and within 24 hours of awareness. Qualified providers: Art 24(2)(fb) uses without undue delay and within 24 hours of the incident. Notify the supervisory body and other recipients required by the provision. Check NIS2 and GDPR separately; these are provider duties. eIDAS Art 19a(1)(b) · eIDAS Art 24(2)(fb)
DSA Specified suspected criminal offence	Hosting providers must promptly inform the relevant law enforcement or judicial authority under Article 18 where the statutory life-or-safety trigger is met. This is separate from cybersecurity incident reporting. DSA Art 18(1)-(2)

Operational rule: Record product versions, support status, users affected, protective steps and what information remains sensitive. Have Legal and the product owner align regulatory and customer communications. Add contractual, insurance and other sector notices to the same timeline.

Legal anchors [CRA Art 14](#) | [CER Art 15](#) | [AI Art 73](#) | [AI amendment](#) | [eIDAS](#) | [DSA Art 18](#)

Use one supplier and procurement gate

Apply the gate at selection, renewal and material change. Scale effort to service impact, data, access and legal role, rather than spend alone. Require extra scrutiny for a small supplier with privileged access to critical systems.

Decision	Ask the supplier or owner	Evidence to obtain
Scope and impact	Which entity supplies the service? What business function, data and systems depend on it? Supports: DORA Art 28(3)-(4) · GDPR Art 28(1)	Service description, locations and dependency map.
Access and data	Who can administer it? Which subprocessors or locations handle data? How are access and deletion controlled? Supports: GDPR Art 28(2)-(3) · GDPR Art 44	Access model, processing terms and data-flow answers.
Security and resilience	What is tested? What exclusions remain? Can the supplier recover within our business needs? Supports: NIS2 Art 21(2)(d) · DORA Art 28(4)(c)-(d)	Relevant assurance report, open findings and recovery evidence.
Incident cooperation	How quickly will we be told, by whom, with what facts? Is support available outside office hours? Supports: GDPR Art 28(3)(f) · DORA Art 30(2)(f), (3)(b)	Negotiated notice obligations and tested contact route.
Audit and change	Can we obtain evidence? What changes, subcontractors or service interruptions must be notified? Supports: GDPR Art 28(3)(h) · DORA Art 30(2)(a), (3)	Contract terms, change rights and responsibility matrix.
Exit and portability	Can we export usable data, transition service and confirm deletion? What time, cost and dependencies remain? Supports: DORA Art 28(8) · Data Act Art 25(2)	Exit plan, sample export and termination terms.
Law-specific terms	Is GDPR processing involved? Does DORA apply to the customer? Are Data Act, AI or product duties relevant? Supports: GDPR Art 28(3) · DORA Art 30(2)-(3) · Data Act Art 25	Completed conditional legal checklist.

Make an explicit approval decision

Approve; approve with dated conditions; or reject/pause. Attach unresolved gaps, compensating measures, accountable business owner and review date. Escalate any mandatory contract or legal requirement that cannot be met.

Acceptance test

Select a critical supplier. Call its escalation route, inspect the assurance report's scope, export representative data and identify one viable continuity or exit option. Record failures as actions rather than filing the questionnaire as complete.

Legal anchors [GDPR Art 28](#) | [NIS2 Art 21](#) | [DORA Arts 28 to 30](#) | [Data Act Chapter VI](#)

Deliver the first 90 days

This is a suggested implementation plan. Any applicable legal deadline, active incident or critical exposure takes priority. Start overdue legal duties immediately rather than scheduling them for a later phase.

When	Work package	Accountable lead	Acceptance criteria
Days 1 to 10	Confirm entity and activity scope. Identify applicable national laws, authorities and reporting obligations. Supports: NIS2 Art 2 · GDPR Art 3 · DORA Art 2	Executive sponsor and Legal	Every priority entity has a reviewed scope record or a dated unresolved issue.
Days 1 to 15	Fix urgent access and exposure gaps; verify critical backups and incident contacts. Supports: NIS2 Art 21(2)(c) , (i)-(j) · NIS2 Art 23	CIO and CISO	Critical exposures have fixes or authorised safeguards; reporting route is usable.
Days 11 to 30	Assign control and law owners. Build the evidence index and prioritised action register. Supports: NIS2 Art 20(1) · DORA Art 5(2)(c) · GDPR Art 24(1)	Programme owner	Every priority gap has one owner, due date and closure test.
Days 16 to 45	Review critical suppliers and personal-data flows. Classify AI and product activities. Supports: DORA Art 28(4) · GDPR Art 30 · AI Act Art 6 · CRA Art 2	Business and specialist owners	Relevant contracts, classifications and operational gaps are recorded.
Days 31 to 60	Implement priority controls; test recovery, privileged access and reporting. Supports: NIS2 Art 21(2)(f) · DORA Art 11(6)	Service owners	Tests produce actual results; failures have funded corrective actions.
Days 61 to 75	Retest fixes. Sample evidence and review national or regulatory changes. Supports: NIS2 Art 21(2)(f) · DORA Art 6(5)-(6)	Assurance and Legal	Closure decisions are backed by evidence; applicability is current.
Days 76 to 90	Management reviews remaining risk, resources and the next quarter. Supports: NIS2 Art 20(1) · DORA Art 5(2)(g)	Executive sponsor	Decisions, budget, next milestones and unresolved legal issues are explicit.

Prioritisation rule

Priority 1: active legal breach, imminent reporting deadline or critical operational exposure. Priority 2: material control gaps affecting important services or people. Priority 3: improvements after the first two categories are controlled. Reclassify when facts change.

Report decisions rather than activity counts

Show what can fail, which obligation is affected, who owns the correction, when it will be tested and which decision management must make. A large number of policies or completed training sessions alone does not establish operating effectiveness.

Reusable scope and authority records

Copy these fields into your existing register. Create one scope record per relevant entity and activity; attach the evidence and reviewer decision. Bracketed fields are intentional blanks for your team to complete.

Recommended records support: [NIS2 Art 2](#) · [NIS2 Art 23\(4\)](#) · [GDPR Art 33\(3\)](#)

Scope record

Field	Complete this
Record and subject	[Record ID] [Legal entity] [Country] [Activity or product]
Business and legal role	[Service and customers] [EU connection] [Controller/provider/deployer or other role]
Legal basis	[Law] [Article] [National implementing law link] [Version checked]
Facts and conclusion	[Size and sector facts] [Exception analysis] [Applies now / later / no / unresolved]
Effective dates	[Duty begins] [Registration deadline] [Designation receipt if relevant]
Decision and review	[Owner] [Legal reviewer] [Approval date] [Next review] [Change trigger]

Authority and reporting card

Field	Complete this for each route
Route and trigger	[Entity] [Law] [Threshold source] [Clock start and time limit]
Authority	[Authority or CSIRT name] [Official portal URL] [Telephone fallback]
People	[Submitter and mobile] [Deputy and mobile] [Approver and escalation]
Access and submission	[Account custodian] [Authentication method] [Template location] [Receipt location]
Test	[Last access test date] [Result] [Unresolved issue and owner]

Before marking the record complete

- Legal has reviewed the exact entity, role, national rule and effective date.
- The submitter and deputy can access the portal; fallback contacts are available offline.
- Credentials are stored in an approved vault, not in this record.

Quality check: Use an unresolved status where the facts are missing. Assign an owner and deadline instead of assuming the activity is exempt.

Reusable action and evidence records

Use one action record per gap and link it to the applicable requirement and control. Keep sensitive evidence in controlled locations; the register should point to it rather than duplicate it.

Record field	What to enter
Requirement and gap	[Action ID] [Entity] [Law and article] [Specific gap and impact]
Action and ownership	[Action] [Named accountable owner] [Delivery team] [Priority] [Due date]
Temporary treatment	[Compensating control] [Approval] [Expiry] [Legal permissibility checked]
Closure test	[Population and method] [Expected result] [Test date] [Reviewer]
Evidence and status	[Evidence link] [Scope and period] [Actual result] [Open / underway / tested / closed]

Worked example

Gap: privileged supplier access to a critical service lacks strong authentication. Action: enforce approved authentication and remove unused accounts. Owner: identity service owner. Closure: test each access path and reconcile the active-account list. Evidence: dated configuration export, test results and approved exceptions. Link to the specific applicable security requirement; do not label the whole law satisfied.

Recommended records and targets support: [NIS2 Art 21\(2\)\(f\)](#) · [DORA Art 6\(5\)-\(6\)](#) · [GDPR Art 24\(1\)](#)

Monthly management dashboard

Measure	Suggested target	Escalate when
Priority entities with approved scope	100% of priority scope	A regulated activity is unresolved or overdue.
Overdue Priority 1 actions	0	Any action remains overdue.
Critical services passing recovery tests	100% of scheduled tests	A service fails its agreed recovery objective.
Critical access paths meeting the standard	100% or approved time-limited treatment	An exposed path lacks adequate safeguards.
Reporting routes with tested access and deputy	100% of applicable routes	A required route cannot be used.
Closed actions with independently checked proof	100% of sampled closures	A closure relies only on a policy or assertion.

Targets above are management recommendations, not legal safe harbours. Define denominators, reporting period and evidence sources. Keep the legal duty, control coverage and operating test result separate.

Track dates and source changes

Legal reference date: 8 October 2026. Review legal changes and national implementation before a consequential scope or reporting decision. Preserve the version and effective date used in the legal register.

Instrument	Date or trigger	Practical action
NIS2	EU transposition deadline was 17 October 2024.	Confirm current national law, entity registration and local reporting rules. NIS2 Art 41(1)
DORA	Applicable since 17 January 2025.	Operate the framework and current technical standards now. DORA Art 64
CRA	Reporting since 11 September 2026; main requirements 11 December 2027.	Run Article 14 reporting now; plan product conformity and lifecycle evidence. CRA Art 71 · CRA Art 69(3)
AI Act	General application 2 August 2026, with phased and amended exceptions.	Operate applicable literacy, prohibited-practice, GPAI and transparency duties. 2026/1744 Art 1(40) · AI Act amended Art 4(1)
AI Act high risk	2 December 2027 for relevant Annex III duties; 2 August 2028 for Annex I duties.	Use amended Article 113 and check legacy-system transitions. 2026/1744 Art 1(40)
AI Act transition	Specified new prohibitions and an existing-system marking transition: 2 December 2026.	Review the exact Article 5 and Article 50 scope under the amendment. AI Act amended Art 111(4) · 2026/1744 Art 1(40)
Data Act	General application 12 September 2025. Article 3(1) covers products and related services placed after 12 September 2026.	Review access-by-design obligations for new products. Data Act Art 50
Data Act switching	Switching charges removed from 12 January 2027.	Review exit terms; distinguish other permitted charges. Data Act Art 29(1)
CER and eIDAS	CER deadlines depend on designation notice. Wallet obligations depend on role and implementing acts.	Record actual triggers and applicable deadlines; avoid a single group-wide date. CER Art 6(3) · CER Art 12(1) · eIDAS Art 5a(1) · eIDAS Art 5f

Supplementary official sources

Legal anchors [NIS2 implementing Regulation 2024/2690](#) | [DORA reporting Regulation 2025/301](#) | [AI amendment 2026/1744](#) | [eIDAS amendment 2024/1183](#)

GDPR and DSA are already generally applicable. Add national and sector rules beyond these nine instruments where relevant. Official texts govern; this guide's owners, tests and delivery plan provide a practical way to implement the assessed requirements.