ITSAILOR FIELD GUIDE

DORA and NIS2: The Strategic IT Roadmap

An executive briefing for ICT risk owners and regulated operators.

2026 EDITION

CIOS

ITSailor

ABOUT THIS GUIDE

DORA and NIS2 move ICT resilience from a technical concern to a management-board responsibility. The question a regulator asks is no longer "do you have a policy" but "can you prove the control runs, who owns it, and how fast you recover".

This briefing maps the obligations to decisions an executive actually makes: scope, framework, incident reporting timelines, resilience testing, third-party concentration and an evidence system that survives an audit.

The output is a sequenced plan with owners and dates, in the language each reviewer expects.

WHO IT IS FOR

CIOs, CTOs, CISOs, founders, legal counsel and compliance owners who carry ICT risk accountability.

WHAT YOU GET

- 12-chapter executive roadmap across DORA and NIS2.
- Article-to-reality matrix mapping obligations to operational work.
- Incident reporting timeline aid (DORA major-incident path; NIS2 24h / 72h / 1 month).
- ICT third-party register and exit-strategy starter structure.
- Board briefing and accountability pack outline.
- 90 / 180 / 365-day prioritised roadmap with a decision matrix.

Michal Jatczak, a Polish engineer based in Malta, trading as ITSailor, a Microsoft Authorized Partner.
Strategic and technical guidance only, not legal advice. DORA is a directly applicable EU Regulation; NIS2 is a Directive transposed into national law, so detail varies by Member State. Confirm scope and obligations with qualified counsel before relying on this roadmap for a regulatory submission.

Free edition. You may share this PDF unchanged; do not sell it or pass it off as your own.

Contents

01	The Regulatory Reality	4
02	Are You In Scope?	6
03	The ICT Risk Management Framework	8
04	Incident Management and the Reporting Clock	10
05	Proving It: Digital Operational Resilience Testing	12
06	Third-Party and Concentration Risk	14
07	The NIS2 Risk-Management Measures	16
08	Governance and Board Accountability	18
09	Building the Evidence System	20
10	Build, Buy or Outsource	22
11	The Board Briefing Pack	24
12	The 90 / 180 / 365-Day Roadmap	26
	Sources and references	28

CHAPTER 1

The Regulatory Reality

DORA and NIS2 turn ICT resilience into management accountability, not a technical side project.

DORA (REGULATION (EU) 2022/2554) **NIS2 (DIRECTIVE (EU) 2022/2555)**

For a decade, ICT risk lived in a register that nobody on the board read. DORA and NIS2 end that arrangement. DORA became applicable on 17 January 2025 for financial entities in scope. NIS2 had a Member State transposition deadline of 17 October 2024 and widens both the sectors covered and the personal accountability of senior management. The shared message is blunt: operational resilience is now a governed outcome that leadership owns and must be able to prove.

The two frameworks come from different places and meet in the same operational reality. DORA is a directly applicable Regulation aimed at the financial sector and the ICT providers it depends on. NIS2 is a Directive, transposed into national law, aimed at essential and important entities across many sectors. If your business touches finance and runs critical infrastructure, you can be inside both. The work does not double; the evidence has to speak two dialects.

EXECUTIVE POSITION

The regulator is not buying your intentions. The defensible answer to every obligation is the same shape: show the control, show the log, show the owner, show the recovery path. A binder of policies is the start of the conversation, not the end of it.

DIMENSION	DORA	NIS2
Instrument	Regulation, directly applicable	Directive, transposed nationally
Primary scope	Financial entities and critical ICT third-party providers	Essential and important entities across listed sectors
Headline shift	Digital operational resilience as a supervised discipline	Management accountability and supply-chain security
Applied / due	Applicable 17 January 2025	Transposition due 17 October 2024

WHY THE BOARD NOW CARES

NIS2 backs its measures with real consequences. Article 34 provides for administrative fines of up to EUR 10 million or 2% of total worldwide annual turnover for essential entities, and up to EUR 7 million or 1.4% for important entities, whichever is higher, as transposed nationally. It also opens the door to holding management personally accountable. ICT risk moved from an IT line item to a board liability.

YESTERDAY	UNDER DORA AND NIS2
Security owned by IT	Risk owned and answered for by the management body
Policy as the deliverable	Evidence the policy runs as the deliverable
Incidents handled quietly	Significant incidents reported on a fixed clock
Vendors chosen on price	Vendors governed for concentration and exit
Resilience asserted	Resilience tested and recorded

This book treats the two as one programme with two reporting languages. The chapters follow the order an operator actually works in: confirm scope, build the risk framework, get incident reporting right, prove resilience by testing, control third-party concentration, satisfy the NIS2 measures, fix governance, and then assemble the evidence system and the roadmap.

EVIDENCE TO KEEP

- A one-page scope statement: which entity, which framework(s), which competent authority.
- A named executive owner for the resilience programme.
- A decision log that records why each obligation applies or does not.

CHAPTER 2

Are You In Scope?

Scope is the first and most expensive mistake. Get it wrong and you either over-build or sit exposed.

DORA ART. 2 | NIS2 ART. 2-3, ANNEXES I-II | NIS2 SIZE-CAP RULE

Before any control work, answer one question precisely: which framework applies to which legal entity. DORA names categories of financial entities (among them credit institutions, payment and e-money institutions, investment firms, insurers and crypto-asset service providers) and extends to the ICT third-party providers they rely on, with a dedicated oversight regime for those designated critical. NIS2 applies to essential and important entities in the sectors listed in its Annexes, generally above defined size thresholds, with some entities in scope regardless of size.

> **THE SIZE-CAP DEFAULT**
>
> NIS2 generally uses a size threshold (broadly, medium and large organisations) to decide who is in scope, with sector-specific exceptions that pull smaller entities in. Member State transposition can adjust the edges, so the national law is the authority, not the Directive alone.

Two traps are common. The first is assuming a group-level answer covers every subsidiary; scope is assessed per entity and per Member State. The second is forgetting the provider side: if you are an ICT provider to a financial entity, DORA reaches you through your client contracts even though you are not a financial entity yourself.

YOU ARE...	LIKELY DORA POSITION	LIKELY NIS2 POSITION
A regulated financial entity	In scope directly	Possibly, by sector
An ICT provider to financial entities	Reached via contractual provisions; possibly a critical provider	Possibly, if in a listed sector and above size cap
A medium/large operator in a NIS2 sector	Usually not, unless financial	In scope as essential or important
A small entity in a critical sub-sector	Generally not	Possibly, despite size, by national rule

A WORKED EXAMPLE

A payments business runs a Maltese parent and a German subsidiary. The parent is a financial entity, so DORA applies to it directly. The German subsidiary also processes for a hospital network, putting it inside a NIS2 supply chain in its Member State. One group, two regimes, two competent authorities. Treated as a single question, the answer is wrong for one of them.

COMMON SCOPE ERROR	CONSEQUENCE	FIX
Answering at group level	A subsidiary sits unprotected or unregistered	Assess per legal entity and Member State
Ignoring the provider side	DORA reaches you through client contracts unaware	Map every contract where you serve a financial entity
Assuming "too small to matter"	A sector rule pulls you in despite size	Check the national transposition, not just the Directive
One-time assessment	A new product silently changes scope	Set reassessment triggers

SCOPE DETERMINATION OUTPUT

- ✓ Entity-by-entity scope statement with the legal basis for each answer.
- ✓ Identified competent authority and registration status for each in-scope entity.
- ✓ List of contracts where you are the ICT provider to an in-scope financial entity.
- ✓ A counsel sign-off line on the final scope determination.

EVIDENCE TO KEEP

- Scope determination memo with legal references per entity.
- Registration confirmation with the relevant national authority where required.
- Reassessment trigger list (new product, new entity, new Member State).

CHAPTER 3

The ICT Risk Management Framework

DORA wants one coherent framework, not a folder of disconnected controls.

DORA ART. 5-15 | ISO/IEC 27001:2022 | NIS2 ART. 21(2)(A)

DORA Articles 5 to 15 require a documented ICT risk management framework with real governance behind it. It is built on familiar pillars: identify your important business functions and the ICT assets behind them; protect them; detect anomalies; respond and recover; and learn from incidents and tests. The difference from a generic ISO programme is the supervisory expectation that the framework is owned at management-body level and demonstrably operates.

Start with the dependency map, not the control list. You cannot protect what you have not connected to a business outcome. For each important function, record the systems, data, identities and third parties it relies on, and the maximum tolerable disruption. That single artefact drives recovery objectives, testing priorities and third-party scrutiny for the rest of the programme.

FRAMEWORK PILLAR	DORA ANCHOR	WHAT "DONE" LOOKS LIKE
Governance	Art. 5	Management body approves the framework and reviews it on a defined cadence
Identify	Art. 8	Asset and dependency map tied to important business functions
Protect and prevent	Art. 9	Access control, encryption, change control, segregation in evidence
Detect	Art. 10	Monitoring and anomaly detection with defined alert ownership
Respond and recover	Art. 11-12	Continuity and recovery plans, backups, tested restore
Learn and evolve	Art. 13	Post-incident review feeding documented improvements

> **THE GOVERNANCE TEST**
>
> If your management body cannot describe the top three ICT risks to the business and the state of their controls, the framework is documentation, not governance. Supervisors increasingly probe the board, not just the security team.

Recovery objectives are a business decision, not a technical guess. Run a short business impact analysis: for each important function, ask how long it can be unavailable before the harm becomes material, and how much data loss is tolerable. The answers become your recovery-time and recovery-point objectives, and they justify every later spend on backup and failover.

TIER	EXAMPLE FUNCTION	INDICATIVE RTO	INDICATIVE RPO
1 - Critical	Core transaction processing	1 hour	5 minutes
2 - Important	Customer portal, reporting	4 hours	1 hour
3 - Standard	Internal analytics	24 hours	24 hours

FRAMEWORK EVIDENCE

- ✓ Management-body approval record with review dates.
- ✓ Asset and dependency register linked to important business functions.
- ✓ Recovery objectives (RTO/RPO) per important function with the basis for each.
- ✓ Control catalogue mapped to DORA Art. 9 and ISO 27001 Annex A.

EVIDENCE TO KEEP

- Board-approved ICT risk framework with version history.
- Dependency map signed off by business and ICT owners.
- RTO/RPO table derived from a business impact analysis, not a guess.

CHAPTER 4

Incident Management and the Reporting Clock

When an incident hits, the timeline is unforgiving. The runbook has to exist before, not during.

DORA ART. 17-19 NIS2 ART. 23

Both frameworks require you to detect, classify and report significant ICT incidents, and both run on clocks that start the moment you become aware. DORA Articles 17 to 19 require a management process for ICT-related incidents and the reporting of major incidents to your competent authority. NIS2 Article 23 sets explicit deadlines for significant incidents that are now the most quoted numbers in the regime.

STAGE	NIS2 ART. 23 DEADLINE	PURPOSE
Early warning	Within 24 hours of awareness	Flag a significant incident, even before full assessment
Incident notification	Within 72 hours	Initial assessment, severity, indicators of compromise
Final report	Within one month	Root cause, mitigation, lessons learned

The DORA major-incident path follows the same logic of initial, intermediate and final reporting to the financial competent authority, against classification criteria set in the regime. The detail differs; the operational requirement is identical. You need a triage that fires fast, a classification you trust, and a named person who can file the early notification without convening a committee.

> **THE 24-HOUR PROBLEM**
>
> Twenty-four hours is not enough time to invent a process. The early warning has to be a button, not a project. Pre-write the templates, pre-assign the filer, pre-agree the threshold. Practise it in a tabletop before a real incident forces the first attempt.

ASPECT	DORA MAJOR INCIDENT	NIS2 SIGNIFICANT INCIDENT
Who reports	Financial entity to its financial competent authority	Essential/important entity to the CSIRT or competent authority
First step	Initial notification on the regime timeline	Early warning within 24 hours
Follow-up	Intermediate report, then final report	Notification within 72 hours, final within one month
Trigger	Major incident classification criteria	Significant incident criteria

A WORKED 24-HOUR TIMELINE

At 02:14 monitoring flags mass failed logins. By 02:40 the on-call confirms a credential-stuffing wave against the customer portal. The incident commander declares at 02:55 and the pre-named filer submits the early warning at 03:30, well inside 24 hours, using a template that already existed. The 72-hour notification and the one-month report follow the same prepared path. Nothing here was invented during the incident.

INCIDENT READINESS PACK

- ✓ Severity and significance classification criteria, written and agreed.
- ✓ Pre-drafted early-warning and notification templates per authority.
- ✓ Named filer and backup, with authority to submit.
- ✓ Evidence-preservation step built into the response runbook.
- ✓ Tabletop exercise on the 24h / 72h / 1 month path, with a date.

EVIDENCE TO KEEP

- Incident classification policy with worked examples.
- Tabletop exercise report against the reporting timelines.
- A reporting log template capturing each deadline and who met it.

CHAPTER 5

Proving It: Digital Operational Resilience Testing

Resilience you have not tested is a claim. DORA wants the claim proven on a schedule.

DORA ART. 24-27 | NIS2 ART. 21(2)(F)

DORA Articles 24 to 27 require a digital operational resilience testing programme, proportionate to the entity, covering tools and systems that support important functions. Tests range from vulnerability assessments and scenario-based testing to, for entities so designated, threat-led penetration testing (TLPT). The point is not the test for its own sake; it is the documented evidence that recovery and defence work under realistic conditions.

> **TLPT IS TARGETED, NOT UNIVERSAL**
>
> Threat-led penetration testing applies to entities identified under the regime, on a periodic basis, and is a heavyweight exercise involving real threat intelligence and red-teaming. Most entities run the broader testing programme; not all are required to run TLPT. Confirm your designation before scoping a TLPT budget.

The most common audit finding in this area is the untested backup. A restore that has never been executed is a hope, not a control. Schedule restore drills, scenario tests and tabletop exercises, run them, and keep the evidence. The schedule and the results matter as much as the tooling.

TEST TYPE	CADENCE (SET TO YOUR RISK)	EVIDENCE PRODUCED
Vulnerability assessment	Continuous / quarterly	Findings, remediation status, retest proof
Backup restore drill	Quarterly	Restore time, data integrity check, sign-off
Scenario / tabletop	Twice yearly	Exercise report, action items, owners
Full failover	Annual	Recovery against RTO/RPO, gaps logged
Threat-led penetration test	Per designation	Scoped report, remediation plan, retest

MATURITY	WHAT IT LOOKS LIKE
Absent	Backups configured, never restored; "we assume it works"
Reactive	Tests run only after an incident or an audit request
Scheduled	A calendar of vulnerability scans, restore drills and tabletops
Evidenced	Every test produces a dated report with findings tracked to closure
Threat-led	Designated entities run TLPT against real threat intelligence

THE BACKUP THAT WAS NEVER RESTORED

A common and avoidable failure: nightly backups ran green for two years, but the first real restore attempt, during an incident, took eleven hours and lost a day of data because nobody had ever measured it. A single quarterly restore drill would have surfaced both problems while they were cheap to fix.

TESTING PROGRAMME OUTPUT

- ✓ A written, risk-based testing plan with a calendar.
- ✓ Restore drill evidence for every important function.
- ✓ Findings tracked to closure with retest proof.
- ✓ Confirmation of whether TLPT applies to you, with the basis.

EVIDENCE TO KEEP

- Annual testing plan approved by the risk owner.
- Restore and failover test reports with measured times.
- Remediation tracker showing findings closed and retested.

CHAPTER 6

Third-Party and Concentration Risk

Your resilience is only as strong as the provider you cannot see and cannot leave.

DORA ART. 28-30 | NIS2 ART. 21(2)(D)

DORA Articles 28 to 30 put ICT third-party risk at the centre. You must keep a register of contractual arrangements for the use of ICT services, ensure key contractual provisions are present, assess concentration risk, and hold a credible exit strategy for arrangements that support critical or important functions. Providers designated as critical ICT third-party providers fall under a direct EU oversight framework.

> **THE EXIT STRATEGY YOU DO NOT HAVE**
>
> Most organisations cannot answer "what happens if this provider fails or we must leave in 90 days". DORA expects a documented, tested exit strategy for arrangements behind critical functions. An exit strategy that has never been rehearsed is a paragraph, not a plan.

Concentration risk is the quiet danger. If three critical functions all sit behind the same cloud region, the same identity provider or the same single vendor, a single failure cascades. The register is not a procurement formality; it is the input to a concentration analysis the board should see.

CONTRACT ELEMENT	DORA EXPECTATION	WHY IT MATTERS
Service and data location	Specified, with sub-processors	Sovereignty, residency and audit reach
Access and audit rights	Granted to entity and authority	You can inspect and so can the regulator
Incident cooperation	Defined notification and support	You meet your own reporting clock
Exit and transition	Documented exit support	You can leave without losing the function
Sub-outsourcing	Controlled and transparent	Hidden fourth parties do not break the chain

REGISTER FIELD	WHY IT EARNS ITS PLACE
Function supported and criticality	Tells you which arrangements need the full treatment
Data location and sub-processors	Drives residency, sovereignty and audit reach
Substitutability	How hard it would be to replace this provider
Exit trigger and exit owner	Turns "we should leave" into an executable plan
Linked Member State and authority	Maps the arrangement to the right oversight

CONCENTRATION, WORKED

Three "different" SaaS tools turn out to run in the same cloud region, authenticate through the same identity provider, and back up to the same object store. On paper that is three vendors. In a failure it is one. The register exists to make that single point of failure visible to the board before an outage does.

THIRD-PARTY CONTROL OUTPUT

- ✓ Register of ICT contractual arrangements, kept current.
- ✓ Concentration analysis across critical functions.
- ✓ Exit strategy for each critical-function provider, with a rehearsal date.
- ✓ Contract gap list against the DORA key provisions.

EVIDENCE TO KEEP

- ICT third-party register with criticality flags.
- Board-level concentration risk summary.
- Exit-strategy documents and the date each was last tested.

CHAPTER 7

The NIS2 Risk-Management Measures

NIS2 Article 21 is a baseline of ten measures. Treat it as the floor, evidenced, not aspired to.

NIS2 ART. 21(2)(A)-(J)

NIS2 Article 21(2) sets out the minimum risk-management measures essential and important entities must take, on an all-hazards basis and proportionate to risk. They overlap heavily with DORA and with ISO 27001, which is the good news: one well-built control system produces evidence for all three. The measures are explicit, so the audit question is simply whether each one is implemented and provable.

NIS2 ART. 21(2) MEASURE	OPERATIONAL TRANSLATION
(a) Risk analysis and information system security policies	A maintained, owned risk and security policy set
(b) Incident handling	The detection, response and reporting machinery from Chapter 4
(c) Business continuity, backup and crisis management	Tested continuity and recovery from Chapter 5
(d) Supply-chain security	The third-party control from Chapter 6
(e) Security in acquisition, development and maintenance	Secure SDLC, vulnerability handling and disclosure
(f) Policies to assess effectiveness	The testing and review programme that proves controls work
(g) Cyber hygiene and training	Baseline practices and recurring awareness training
(h) Cryptography and encryption	A cryptography policy with key management
(i) Human resources, access control, asset management	Joiner/mover/leaver, least privilege, asset register
(j) MFA, secured communications and emergency comms	MFA enforced, secured voice/video/text, fallback comms

THE CHEAPEST HIGH-IMPACT MEASURE

Measures (i) and (j) - access control and multifactor authentication - are low cost and stop the majority of real-world compromises. If budget is tight, this is where evidence and risk reduction line up most cleanly.

Proportionality is the operative word. A 40-person important entity is not expected to run the same programme as a systemic bank. The measures are mandatory, but their depth scales with your size, risk exposure and current good practice. What does not scale away is evidence: even a small entity must be able to show each measure is implemented.

WHERE TO START

If you are building from a low base, the highest return per euro is access control plus multifactor authentication (i and j), incident handling (b), and backup with tested recovery (c). Those four blunt most real attacks and produce evidence other measures depend on. Cryptography and secure development follow once the basics hold.

NIS2 MEASURE EVIDENCE

- ✓ A measure-by-measure status sheet: implemented, partial, or gap, with evidence.
- ✓ Training records with completion rates.
- ✓ Access control and MFA enforcement evidence.
- ✓ A remediation plan for every partial or gap, with owner and date.

EVIDENCE TO KEEP

- Article 21 coverage matrix with evidence links.
- Cryptography and access-control policies in force.
- Supply-chain security documentation cross-referenced to Chapter 6.

CHAPTER 8

Governance and Board Accountability

NIS2 makes management personally answerable. The board cannot delegate the obligation, only the work.

NIS2 ART. 20 | DORA ART. 5 | DORA ART. 13

NIS2 Article 20 requires management bodies to approve the risk-management measures, oversee their implementation, and can hold them accountable for failures. It also requires that management receive training to understand the risks they govern. DORA Article 5 places equivalent weight on the management body for the ICT risk framework. The era of "the IT team handles it" is over in law as well as in practice.

> **ACCOUNTABILITY IS NOT A JOB TITLE**
>
> Appointing a CISO does not transfer the obligation away from the board. The management body approves, oversees and answers for the measures. Training and a regular, substantive review on the agenda are how a board demonstrates it actually governs the risk.

Translate this into a governance rhythm the board can sustain: a standing ICT risk item on the agenda, a concise dashboard the directors actually read, recorded decisions on accepted risks, and evidence that management training happened. The goal is a defensible record that the people accountable in law understood and directed the programme.

CADENCE	BOARD / MANAGEMENT ACTION
Every meeting	A standing ICT-risk item with a one-page dashboard
Quarterly	Review of top risks, open incidents and remediation progress
Annually	Approve the framework, the testing plan and the budget; record training
On event	Major incident and material third-party change escalated to the board

> **THE THIRTY-MINUTE BOARD ITEM**
>
> Accountability does not require the board to become engineers. It requires a recurring, recorded, substantive thirty minutes: here are the top three ICT risks, here is what changed, here is what we decided, here is what we accept. Minuted, that single habit is much of what a supervisor wants to see.

GOVERNANCE EVIDENCE

- ✓ Board minutes approving the risk framework and reviewing it on cadence.
- ✓ Management training records on ICT and cyber risk.
- ✓ An accepted-risk register with named decision owners.
- ✓ A board-readable risk dashboard, versioned over time.

EVIDENCE TO KEEP

- Management-body approval and review minutes.
- Training completion records for directors and senior management.
- Decision log for risk acceptance and major ICT investments.

CHAPTER 9

Building the Evidence System

The programme is judged on what you can show, not what you intended. Engineer the evidence, not just the control.

DORA ART. 6, 13 | NIS2 ART. 21(2)(F) | ISO/IEC 27001:2022

Every chapter so far ends with an evidence list for one reason: an audit is an evidence exercise. The strongest programmes treat evidence as a product. They decide, for each control, what artefact proves it, where that artefact lives, who owns it, and how often it refreshes. When a regulator or auditor asks, the answer is a link, not a fire drill.

CONTROL DOMAIN	PRIMARY EVIDENCE ARTEFACT	REFRESH CADENCE
Identity and access	Policy export, access review record, MFA enforcement proof	Quarterly
Incident management	Classification policy, tabletop report, reporting log	Per incident + twice yearly
Continuity and recovery	Restore test report, RTO/RPO table	Quarterly
Third-party risk	Register, concentration analysis, exit-test record	Quarterly / on change
Governance	Board minutes, training records, decision log	Per meeting

THE OPERATOR DEFINITION OF EVIDENCE

If a control cannot be shown in configuration, logs, change history or a named owner register, it is not evidence yet. A document that asserts a control exists is useful only once the system proves the control runs.

Treat evidence the way you treat a product: it has an owner, a source of truth, a refresh cycle and a consumer. The consumer is a future auditor or regulator under time pressure. Design for that moment now, while it is calm, and an audit becomes a retrieval task rather than a scramble.

FAILED ON RETRIEVAL, NOT ON CONTROL

Organisations rarely fail an audit because the control was missing. They fail because they could not produce the proof fast enough, or the proof was a year stale, or nobody owned it. The control existed; the evidence system did not. That is an avoidable, self-inflicted finding.

EVIDENCE SYSTEM OUTPUT

- ✓ An evidence map: control to artefact to location to owner.
- ✓ A refresh calendar so evidence never goes stale before an audit.
- ✓ A single index an auditor can be handed on day one.
- ✓ A gap list where evidence is asserted but not yet producible.

EVIDENCE TO KEEP

- Evidence index covering every in-scope obligation.
- Refresh schedule with owners.
- A mock audit walkthrough that tests the index end to end.

CHAPTER 10

Build, Buy or Outsource

Most resilience gaps are sourcing decisions made by default. Decide them on purpose, with the regulator in the room.

DORA ART. 28-30 | NIS2 ART. 21(2)(D) | DORA ART. 12

Every control in this book can be built in-house, bought as a product, or outsourced to a provider. The frameworks do not tell you which to choose, but they do change the maths: an outsourced control still has to be governed, evidenced and exitable, and a bought tool you cannot leave is a concentration risk wearing a procurement badge. Make the sourcing call deliberately, function by function, not by whoever sold last.

OPTION	STRENGTH	REGULATORY COST
Build in-house	Full control and knowledge retention	You own all the evidence and the run cost
Buy a product	Speed and maintained capability	Concentration and exit must be governed
Outsource to a provider	Capability without headcount	Full DORA third-party treatment applies
Hybrid	Match each function to the right model	More interfaces to evidence and test

> **THE LOCK-IN THAT FAILS AN AUDIT**
>
> A managed service that holds your data, your configuration and your only copy of the runbook is not a convenience, it is a single point of failure the regulator will ask about. If you cannot describe how you would leave inside a defined window, you do not have a supplier, you have a dependency.

A useful test for any sourcing decision: could a competent engineer who is not us take this over with what we would hand them on day one. If the honest answer is no, the arrangement needs an exit plan before it needs a renewal. Sovereignty of your own operations is the quiet objective behind the third-party rules.

SOURCING DECISION OUTPUT

- ✓ A build/buy/outsource decision recorded per important function, with the reason.
- ✓ For every bought or outsourced control: an owner, an evidence path and an exit trigger.
- ✓ A concentration view across all sourcing decisions, not one contract at a time.
- ✓ A "could someone else run this" test applied to each critical arrangement.

EVIDENCE TO KEEP

- Sourcing decision log mapped to important functions.
- Exit and transferability assessment for each critical supplier.
- Concentration summary that survives a board question.

CHAPTER 11

The Board Briefing Pack

The board cannot govern what it cannot see in ten minutes. Build the pack that makes oversight real and recorded.

NIS2 ART. 20 | DORA ART. 5 | DORA ART. 13

Governance fails in practice when the board is handed forty slides of security telemetry it cannot interpret. Accountability under NIS2 Article 20 and DORA Article 5 needs the opposite: a short, honest pack that lets non-specialist directors understand the top risks, approve the plan, and have their decisions minuted. The pack is the instrument of oversight, and increasingly it is the evidence of it.

SECTION	WHAT IT SHOWS	WHY THE BOARD NEEDS IT
Top risks	The three to five ICT risks that matter, with trend	Lets directors govern the few, not the noise
Posture and gaps	Where controls stand against the framework	Shows what is covered and what is not
Incidents and reporting	Significant incidents and whether clocks were met	Proves the response machinery works
Third-party exposure	Concentration and any critical-supplier change	Surfaces the dependency the board owns
Decisions requested	Approvals, accepted risks, budget asks	Turns a briefing into governance on record

ONE NUMBER THE BOARD SHOULD ALWAYS SEE

Pick a single, honest headline metric and track it every meeting: for example the percentage of important functions with a tested recovery and a current owner. A number that moves, with a story behind it, governs better than a heat map nobody trusts.

THE PACK IS ALSO YOUR EVIDENCE

If a supervisor asks how the board exercised oversight, the answer is this pack and the minutes that record what was decided. A briefing that exists but was never minuted, or minutes with no substance behind them, satisfy neither the spirit nor the letter of the accountability rules.

BRIEFING PACK OUTPUT

- ✓ A one-page risk dashboard the directors actually read.
- ✓ A standing decisions-requested section, so every meeting produces a record.
- ✓ A consistent headline metric tracked over time.
- ✓ Minutes that capture approvals, accepted risks and their owners.

EVIDENCE TO KEEP

- The current board pack plus the last four, to show the trend.
- Minutes recording the decisions taken on each.
- A distribution and confidentiality note for the pack.

CHAPTER 12

The 90 / 180 / 365-Day Roadmap

Sequence beats effort. Bank the high-impact, low-effort controls first, then build the structural ones.

DORA ART. 5-30 NIS2 ART. 20-23

Compliance is not bought in a single quarter, and trying to do everything at once produces shelf-ware. Sequence the work by risk reduced per unit of effort. The first ninety days establish accountability and the incident clock, because those carry the sharpest exposure. The next half year builds the framework, testing and third-party control. The full year closes structural gaps and turns the programme into a repeating cycle.

HORIZON	FOCUS	OUTCOME
0-90 days	Scope, governance, incident reporting, MFA and access	You can prove who is accountable and meet the reporting clock
90-180 days	Risk framework, dependency map, testing programme, register	The framework operates and third-party risk is visible
180-365 days	Exit strategies, concentration fixes, evidence system, full test cycle	A defensible, repeating programme rather than a one-off push

WHERE PROJECTS STALL

Two things sink these programmes: no single accountable owner, and evidence treated as an afterthought. Fix both early. An owner with authority and an evidence system that refreshes itself will carry the programme further than any tool purchase.

ROADMAP OUTPUT

- ✓ A prioritised backlog scored by risk reduced and effort.
- ✓ Named owners and dates for every 0-90 day item.
- ✓ A board-approved budget aligned to the three horizons.
- ✓ A review cadence that turns the roadmap into an annual cycle.

FIRST 90 DAYS - TASK	OWNER	DONE WHEN
Confirm scope and competent authority	Legal + exec sponsor	A signed scope memo exists
Name the accountable owner and brief the board	Management body	Minuted approval recorded
Stand up the incident reporting runbook	Security lead	Templates, named filer and a tabletop done
Enforce MFA and least-privilege access	IT	Enforcement evidence exported
Start the ICT contractual register	Procurement	Critical arrangements logged

WHAT GOOD LOOKS LIKE AT DAY 365

A named owner the board can point to. An incident clock you have rehearsed. A risk framework tied to a dependency map. A testing calendar with real restore evidence. A third-party register with exit strategies for the critical few. And an evidence index an auditor could be handed tomorrow. Not perfect, but defensible, and repeating on its own cadence.

Use this book to brief the board and to sequence the work. The Architecture & Security Design Workshop covers the Microsoft 365 and Azure side of that plan in your own tenant: a tenant evidence register and an Exit Kit written against it. The register of information and the exit strategies DORA asks of your entity stay your own work.

EVIDENCE TO KEEP

- A signed-off 90 / 180 / 365-day plan with owners.
- A board-approved budget mapped to the roadmap.
- A first-quarter status review proving the plan moved.

Sources and references

Regulation (EU) 2022/2554 (DORA) LEGAL

Articles 5-30: ICT risk management, incident reporting, resilience testing, third-party risk. Confirm how it applies to your entity with qualified counsel.

Reviewed 2026-06-26 · **Open primary source**

Directive (EU) 2022/2555 (NIS2) LEGAL

Articles 20-23 and Annexes I-II: governance, risk-management measures, reporting, in-scope sectors. National transposition varies; confirm it with qualified counsel.

Reviewed 2026-06-26 · **Open primary source**

ISO/IEC 27001:2022 STANDARD

Information security control families referenced for cross-mapping.

Reviewed 2026-06-26 · **Open primary source**

The Microsoft 365 side, in your own tenant

Use the guide to brief the board and sequence the work. The Architecture & Security Design Workshop covers the Microsoft 365 and Azure side of that plan in your own tenant.

https://www.itsailor.io/handbook/workshops/architecture-security-design