Paul Reynolds
cyber security simplicity

DORA Gap-To-Action Blueprint

For FinTech And SaaS Vendors

A practical 60-day roadmap to transform regulatory requirements into procurement-ready evidence and commercial advantage.

Paul Reynolds
cyber security simplicity

The Procurement Stall

The Reality

You're two weeks into a promising sales cycle with a major EU bank. Then procurement sends a list of evidence requests you can't assemble overnight. Questions about operational resilience, incident response, and supply chain controls keep circling back.

Meanwhile, your product team juggles feature deadlines, legal negotiates liability language, and security scrambles for archived logs. The deal is slipping.

Common Pain Points

- Unprepared for sudden evidence requests during procurement
- Drawn-out contract negotiations without demonstrable controls
- Compliance work consuming product delivery time
- Same people building product and managing remediation

Paul Reynolds
cyber security simplicity

Why This Matters Now

Regulators and banks aren't just issuing guidance—they're shifting procurement criteria and oversight practices. This directly affects deal velocity and your ability to win institutional customers.

Credibility Gaps

Slow responses create credibility gaps that give buyers negotiation leverage

Commercial Impact

Leverage translates into delayed deals, onerous commitments, or lost opportunities

Market Reality

Buyers favor vendors who demonstrate traceable remediation within weeks, not months

Paul Reynolds
cyber security simplicity

Your 60-Day Blueprint

This ebook provides a clear, pragmatic blueprint to close the gap within a focused 60-day window. You'll gain vendor-centered DORA interpretation, rapid gap analysis methods, sprint-ready remediation roadmaps, and role-specific playbooks.

01

Rapid Gap Analysis

Collect minimal viable evidence and build a gap register mapped to DORA provisions

02

60-Day Roadmap

Convert gaps into weekly sprints with owners and acceptance criteria

03

Evidence Packaging

Create procurement-ready deliverables that pass scrutiny

04

Commercial Positioning

Turn remediation into competitive advantage during negotiations

Paul Reynolds
cyber security simplicity

Built On Real Experience

This approach is founded on hard-learned patterns from dozens of real vendor procurement engagements, contract negotiations, and audit readiness exercises with EU financial institutions.

Buyer-Focused

Emphasizes what buyers actually ask for, not theoretical compliance checklists

Resource-Aware

Recognizes constraints and shows minimal viable controls that demonstrate risk reduction quickly

Implementation-Ready

Provides templates and scripts so teams don't reinvent the wheel

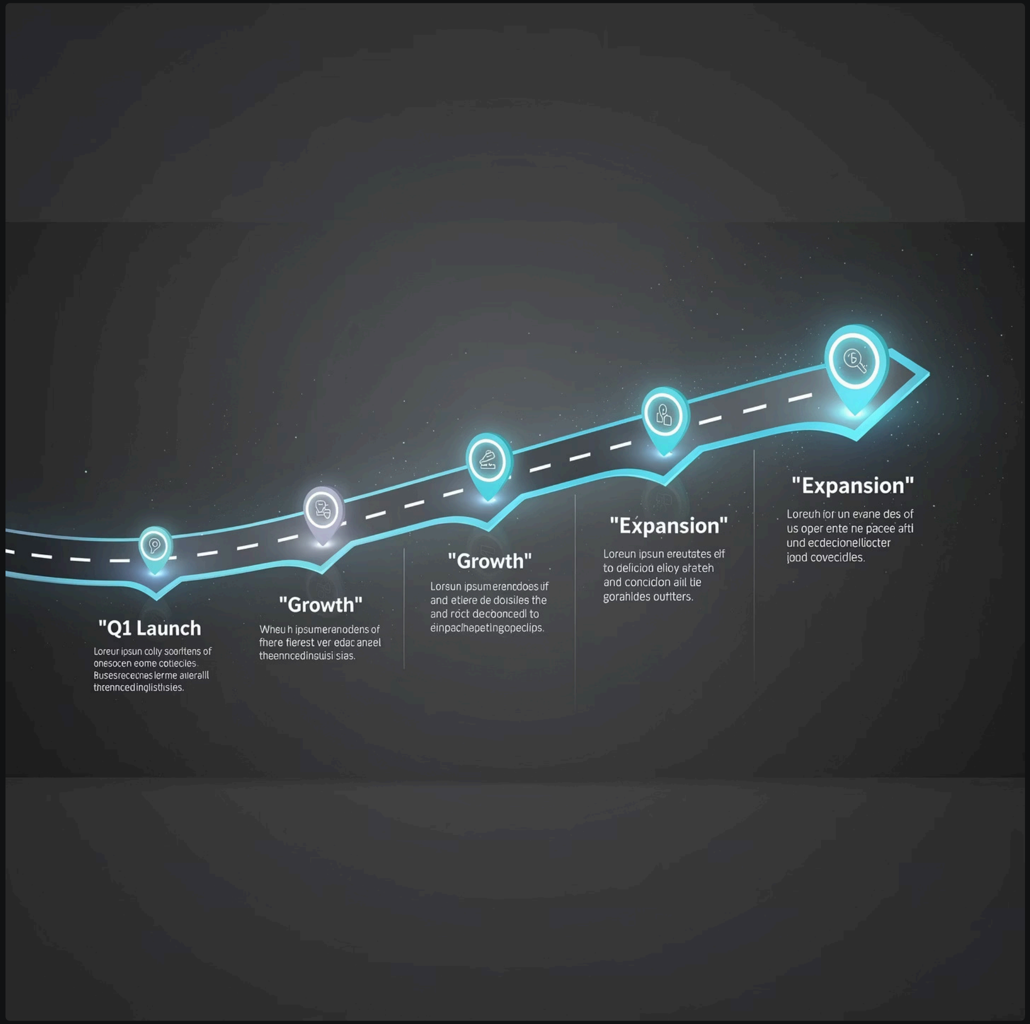
Paul Reynolds
cyber security simplicity

What Makes This Different

Vendor-Centric Approach

Instead of treating DORA as an academic exercise, this framework translates regulatory requirements into concrete buyer questions and acceptance criteria. It prioritizes remediation that removes procurement blockers first.

The process is time-boxed and evidence-driven, emphasizing traceability so every remediation ticket points back to the regulatory clause and procurement question it resolves.



Paul Reynolds
cyber security simplicity

Your Journey Through This Book

1. **Understanding DORA**
   Vendor exposure perspective and supervisory expectations
2. **Gap Analysis**
   Rapid discovery method and gap register creation
3. **60-Day Roadmap**
   Weekly milestones and acceptance criteria
4. **Operational Integration**
   Security, incident response, and third-party risk blueprints
5. **Stakeholder Playbooks**
   Role-based guidance for legal, compliance, product, and sales
6. **Evidence Packaging**
   Audit-ready deliverables and quality checks
7. **Commercial Strategy**
   Procurement positioning and negotiation leverage
8. **Sustaining Resilience**
   Governance rhythms and long-term maturity

Paul Reynolds
cyber security simplicity

How To Use This Book

Use this as a practical workshop guide rather than a reference you read once. Start by scheduling a cross-functional alignment session before beginning gap analysis.

1 Align Teams

Convene product, security, legal, and account teams for initial planning

2 Gather Evidence

Use rapid discovery to collect minimum viable evidence for gap register

3 Execute Sprints

Convert register into weekly sprints with named owners and acceptance criteria

4 Package Results

Create interim evidence packages as living documents that evolve

Paul Reynolds
cyber security simplicity

Imagine The Difference

When the next procurement call lands, instead of scrambling you have a clear status update, prioritized roadmap, and evidence packages that directly answer buyer checklists.

Procurement moves from suspicion to informed confidence. Negotiations focus on commercial terms, not operational uncertainty. Your sales team converts remediation work into a differentiator that underscores reliability.

Outcomes

- Close deals faster
- Reduce contractual risk
- Free engineering capacity
- Make future engagements routine

Paul Reynolds
cyber security simplicity

Understanding DORA And Vendor Exposure

Chapter Introduction

You sell software to banks and payment providers, and a new set of regulatory expectations has started shaping every procurement conversation. This chapter translates the Digital Operational Resilience Act (DORA) into practical concerns that determine whether you close deals or stall in procurement.

You'll learn which DORA provisions matter most to vendors, how supervisory expectations appear in RFPs and due diligence, and how to define focused scope for vendor-centered gap analysis.

Paul Reynolds
cyber security simplicity

The Vendor Challenge

Spotlight Shift

DORA shifts focus from financial institutions alone onto their suppliers, creating new third-party risk expectations

Time Pressure

Procurement processes are time-sensitive—buyers remove vendors from shortlists without clear evidence within weeks

Without a vendor-focused approach, teams spend months compiling documents that don't map to supervisory expectations, costing deals and revenue.

Paul Reynolds
cyber security simplicity

Three Pillars Buyers Care About

Governance & Accountability

Roles, policies, and contractual rights demonstrating board-level risk treatment

Operational Controls & Testing

Continuity plans, incident management, and resilience testing evidence

Third-Party & Contractual Readiness

Subcontractor oversight, audit rights, and reporting processes

Paul Reynolds
cyber security simplicity

Governance & Accountability Evidence

Buyers will ask who is accountable for operational resilience and whether you have policies integrating resilience into product development, change management, and incident response.

Governance Charter

Document defining board or executive oversight structure

Board Minutes

Recent resilience review documentation

Role Descriptions

Named resilience lead with clear responsibilities

Policy Documents

Resilience objectives tied to measurable KPIs

Paul Reynolds
cyber security simplicity

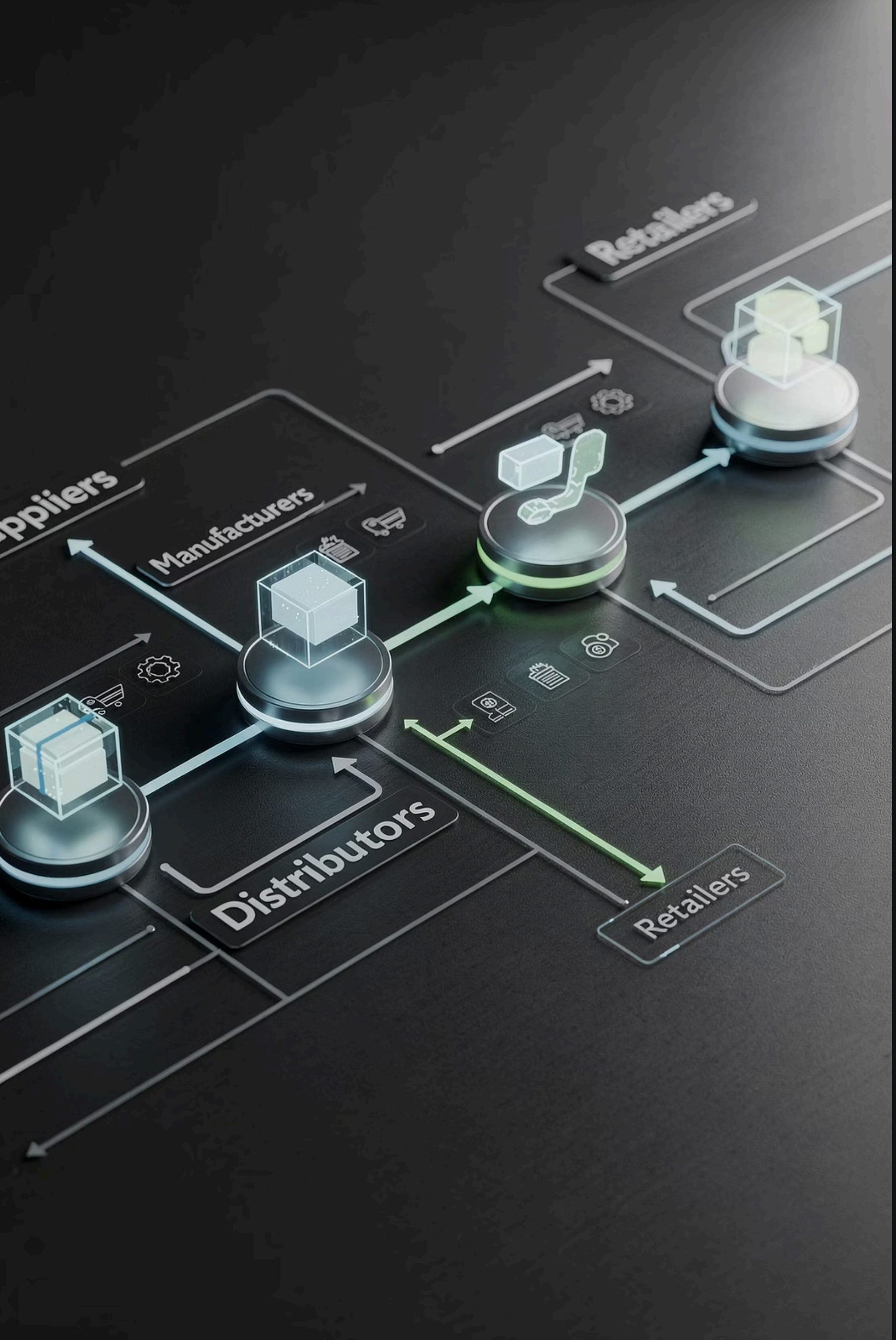
Operational Controls & Testing Evidence

What Supervisors Expect

Supervisors expect vendors to show they can maintain essential services under stress. Buyers will ask if you have continuity plans, whether those plans are exercised, and what testing reports you can share.

Required Evidence

- Tabletop exercise summaries
- Disaster recovery drill results
- RTO and RPO documentation
- Incident logs showing real-world handling
- Failover test results
- Capacity planning evidence



Paul Reynolds
cyber security simplicity

Third-Party & Contractual Readiness

Institutions need comfort that you can manage your own suppliers and provide necessary access for audits or investigations.

Subcontractor Inventory

Complete list with criticality ratings

Contractual Clauses

Standard terms including audit and access rights

Due Diligence Records

Evidence of subcontractor assessment

Notification Templates

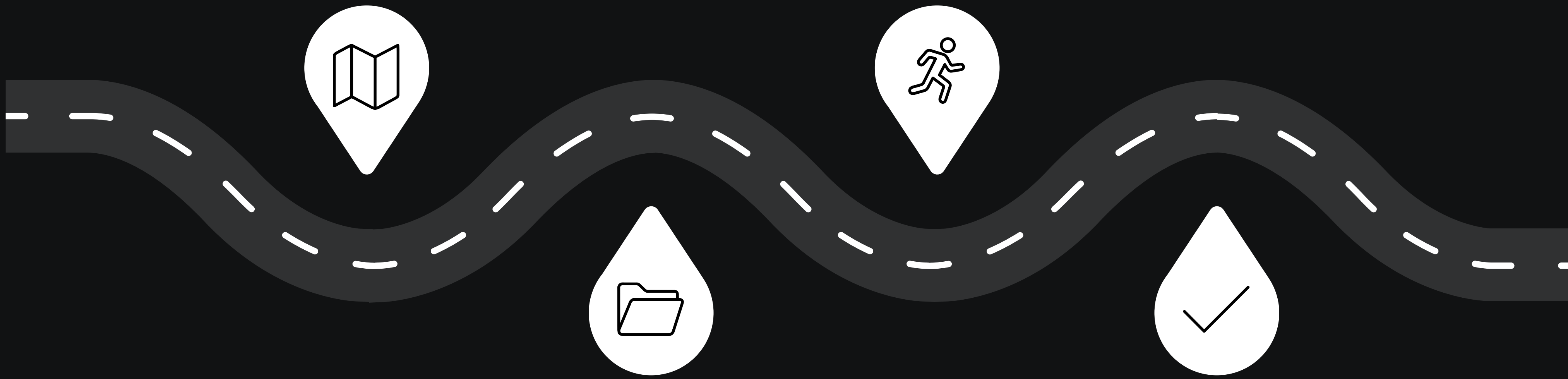
Incident notification clause examples

Paul Reynolds
cyber security simplicity

Your 60-Day Implementation Plan

Scope
Days 0-7: Prioritize critical gaps

Execute
Days 22-40: Run remediation sprints



Collect
Days 8-21: Gather evidence and templates

Validate
Days 41-60: Verify work and share results

This structured approach ensures you close critical gaps while maintaining deal momentum and preserving product delivery capacity.

Paul Reynolds
cyber security simplicity

Real-World Success: Payment Platform

The Challenge

A mid-sized payment platform lost a major bank customer during vendor onboarding due to lack of contractual audit rights and unclear incident timelines.

The Solution

Using the three-pillar framework, the vendor produced a Resilience Brief, updated contract templates to include 24-hour incident notification, and documented a named resilience lead.

Result: Within six weeks they reengaged the buyer and regained qualification in the procurement process.

Paul Reynolds
cyber security simplicity

Running A Targeted DORA Gap Analysis

Chapter Introduction

You're about to learn a focused, practical method to run a high-confidence DORA gap analysis that finishes with an actionable 60-day remediation plan. This chapter provides a compressed discovery playbook tailored to product, security, legal, and operations teams.

You'll get interview templates, minimum viable evidence lists, gap register structures mapped to DORA articles, and prioritization models that translate findings into buyer impact categories.

Paul Reynolds
cyber security simplicity

The Gap Analysis Problem

1

Too Much Documentation

Teams collect excessive raw documentation that never reaches procurement

2

Ambiguous Findings

Findings that legal cannot contract against or operationalize

3

Missing Buyer Impact

No mapping from gaps to procurement consequences

4

Vague Timelines

Remediation priorities not time-bound to 60-day sprint

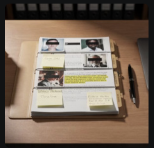
Paul Reynolds
cyber security simplicity

The DORA Gap-to-Action Blueprint

This approach compresses discovery into four coordinated streams, each designed to feed a concise gap register that supports fast remediation.

Targeted Interviews

Collect context and risk signals from five key roles in 45-minute sessions



Minimum Viable Evidence

Demonstrate control existence or intent with representative artifacts

Gap Register

Map to DORA articles and supervisory expectations with clear ownership

Prioritization Heuristics

Translate gaps into buyer impact and 60-day urgency categories

Paul Reynolds
cyber security simplicity

Targeted Interview Framework

Focus interviews on five roles, limiting each session to 45 minutes for maximum efficiency.

Product Owner / Head of Engineering

Architecture, change windows, third-party dependencies

Information Security Lead

Incident detection, logging, security exercises

Operations / SRE Lead

Backups, recovery objectives, operational runbooks

Legal / Compliance Lead

Contracts, SLAs, incident reporting clauses

Vendor Risk Contact

Current due diligence requests, deal blockers

Paul Reynolds
cyber security simplicity

Key Interview Questions

Incident History: Which incidents in the last 24 months required customer notification, and what was the root cause?

Dependencies: Which external service dependencies would prevent service delivery if unavailable for 72 hours?

Playbooks: What documented playbooks exist for incident classification and notification to customers?

Testing Evidence: Where is evidence of tabletop exercises and how were findings tracked to completion?

Paul Reynolds
cyber security simplicity

Minimum Viable Evidence List

Core Artifacts

Require only evidence that proves control intent and recent execution. Focus on representative artifacts, not complete libraries.

- Architecture diagram with critical third parties highlighted
- Incident playbook or runbook for high-severity events
- Sample incident report (redacted for confidentiality)
- Backup and recovery test report with dates and outcomes
- Contractual clauses for incident notification or subprocessor use
- Recent tabletop exercise summary and action items

Paul Reynolds
cyber security simplicity

Gap Register Structure

Use a simple table structure that maps technical findings to business impact and remediation priorities.

Gap ID	Description	DORA Article	Buyer Impact	Owner	Priority
G-001	Missing recovery test evidence	Article 11	Contractual Risk	Ops Lead	High
G-002	No incident notification SLA	Article 17	Procurement Blocker	Legal	Critical
G-003	Subcontractor list incomplete	Article 28	Audit Observation	Procurement	Medium

Paul Reynolds
cyber security simplicity

Prioritization For 60-Day Window

1

Critical: Fix Within 14 Days

Gaps that block procurement outright, such as missing incident notification clauses where contract requires time-bound obligation

2

High: Fix Within 30 Days

Gaps creating material contractual risk or likely audit findings, such as missing recovery tests for critical services

3

Medium: Fix Within 45 Days

Gaps requiring policy updates, tabletop remediation, or small code changes

4

Low: Fix Within 60 Days

Documentation cleanup, process refinements, or longer-term architectural work with interim mitigations

Paul Reynolds
cyber security simplicity

Case Study: SaaS Vendor Success

A mid-size SaaS vendor selling to EU banks followed this blueprint and focused interviews on three customer use cases, producing a minimal evidence set in two weeks.

Discovery

Identified absence of notification SLA and recovery testing gaps for one region

Prioritization

Set notification clause as Critical and scheduled region-specific recovery test in Sprint 1

Outcome

Converted potential procurement blocker into documented remediation commitment with interim evidence

Procurement accepted the interim evidence package while final work was completed, preserving the deal timeline and reducing legal negotiation friction.

Paul Reynolds
cyber security simplicity

Designing The 60-Day Gap-To-Action Roadmap

Chapter Introduction

You completed a targeted DORA gap analysis and now hold a prioritized register pointing to what matters most to buyers and supervisors. This chapter converts that register into a time-boxed 60-day plan you can execute with confidence.

You'll learn how to sequence work for early wins, define minimal viable controls that answer buyer questions, and build traceability from individual tickets back to DORA clauses.

Paul Reynolds
cyber security simplicity

The Roadmap Challenge

What Buyers Demand

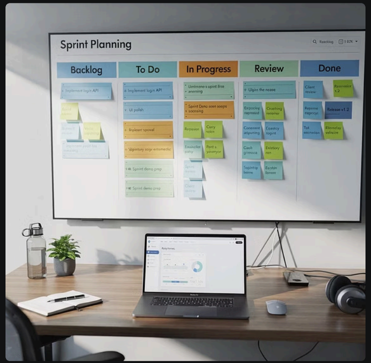
Financial institutions demand clear, verifiable controls and traceable responses to regulatory requirements. Vendors often respond with long roadmaps, vague commitments, or incomplete artifacts.

Three Core Problems

1. Procurement stalls because reviewers cannot validate progress
2. Buyers escalate security or legal concerns, leading to lost deals
3. Teams burn time on low-impact work that doesn't reduce buyer objections

Paul Reynolds
cyber security simplicity

The Gap-to-Action Blueprint Framework

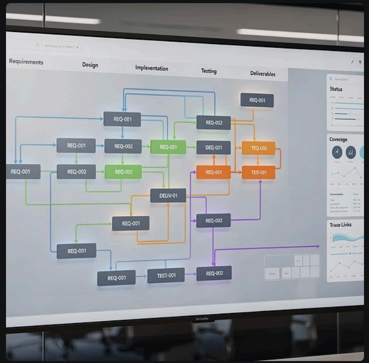


Time-Boxed Sprints

Weekly acceptance criteria create rhythm and visible progress

Minimal Viable Controls

Address buyer objections with smallest change that meets intent



Traceability Matrix

Link each remediation ticket to specific DORA clauses and buyer questions

Interim Evidence Packages

Curated artifacts that procurement and security reviewers can evaluate on rolling basis

Eight-Week Sprint Structure

1

Week 0: Kickoff & Baseline

Assemble squad, confirm gap register, build traceability matrix

2

Week 1: Quick Wins

Deliver two tangible artifacts, create evidence package templates

3

Week 2: Control Implementation

Implement minimal viable control, run end-to-end test, rehearse walkthrough

4

Week 3: Procurement Artifacts

Address SLAs, subprocess documentation, produce interim evidence package

5

Week 4: Consolidation

Consolidate controls, record change approvals, prepare audit memo

6

Week 5: Verification

Complete security verification, produce remediation log and sign-off

7

Week 6: Supplier Evidence

Update onboarding checklist, create supplier evidence pack

8

Week 7: Executive Summary

Prepare consolidated binder, rehearse buyer presentation

9

Week 8: Handover

Deliver final packages, capture feedback, schedule follow-up actions

Paul Reynolds
cyber security simplicity

Minimal Viable Controls Explained

Minimal viable controls are targeted changes that meet regulatory intent without full program rebuilds. They provide rapid risk reduction while permanent solutions are planned.

Example: Vendor Risk

Instead of complete vendor risk program, deploy temporary enhanced onboarding checklist for critical suppliers with documented escalation paths

Documentation

Explain intent and duration of temporary control in evidence package

Roadmap

Schedule permanent control in 90-180 day plan with clear milestones

Paul Reynolds
cyber security simplicity

Operational Integration: Security, Incident Response, And Third-Party Risk

Chapter Introduction

You converted your gap register into a 60-day plan with weekly milestones. Now it's time to make those plans operational, so remediation work becomes repeatable evidence that buys you credibility during procurement and audit reviews.

This chapter provides blueprints to integrate three operational domains that matter most under DORA: security controls, incident response, and third-party risk management.

Paul Reynolds
cyber security simplicity

Three-Pillar Integration Framework

Security Controls

Hardened configuration baselines, access control rules, logging and alerting with configuration snapshots and retention policies

Incident Response

Aligned playbooks, notification timeline templates, tabletop exercise artifacts with documented procedures and test results

Third-Party Risk

Supplier inventory, contract addenda, subprocessor attestations with security questionnaires and compliance documentation

Paul Reynolds
cyber security simplicity

Security Controls Blueprint

Focus on configurations that give auditors quick wins: identity and access, encryption, and observable logging.

1	2	3
Identity & Access Require MFA for all privileged accounts, limit console access to role-based identities, maintain access change log	**Encryption** Ensure encryption in transit with TLS 1.2+, encryption at rest with documented key management	**Logging** Centralize logs with 12+ month retention, create alerts for failed logins, privileged role creation, unusual data exports

These three checks are relatively low effort in cloud-native architectures but address typical procurement red flags.

Incident Response Alignment

Core Elements

An incident playbook in a product team wiki isn't enough. Buyers need to see how operational controls map to detection, escalation, and notification timelines.

- Incident playbook template with escalation matrix
- Notification timeline defining internal and external windows
- Tabletop exercise focusing on realistic scenario

Paul Reynolds
cyber security simplicity

Stakeholder Playbooks: Legal, Compliance, Product, And Sales

Chapter Introduction

You're inside the 60-day sprint to close DORA gaps, and procurement conversations are accelerating. Legal, compliance, product, and sales each handle buyer questions that could stall deals if not tightly coordinated.

This chapter provides role-specific playbooks so each function speaks with one voice, moves remediation forward, and converts regulatory effort into commercial momentum.

Paul Reynolds
cyber security simplicity

Evidence Packaging And Audit-Ready Deliverables

Chapter Introduction

You've done the hard work—mapped gaps to actions and synchronized teams. Now comes the moment that decides whether a buyer sees you as audit-ready or asks for more proof.

This chapter shows how to package evidence into concise, persuasive deliverables that answer procurement and supervisory questions quickly. You'll learn formats, minimum content, and hygiene practices that reduce back-and-forth.

Paul Reynolds
cyber security simplicity

Commercial Positioning And Procurement Strategy

Chapter Introduction

You've spent 60 days closing gaps, producing audit-ready evidence, and briefing stakeholders. Now you face procurement, where legal teams, buyers, and risk officers will test what you've delivered.

This chapter shows how to turn remediation progress into commercial advantage, package commitments so buyers feel comfortable signing, and price and limit liability in ways that reflect operational resilience work under DORA.

Paul Reynolds
cyber security simplicity

Sustaining Resilience Post-60 Days

Chapter Introduction

You just finished an intense 60-day remediation sprint. Immediate fires are contained, buyers are reassured, and attestations are assembled. Now comes the harder work: converting a time-limited push into a durable operating model.

This chapter shows how to move from sprint mode to steady state, so your organization sustains DORA alignment while staying agile and commercially competitive.

Paul Reynolds
cyber security simplicity

Your Path Forward

You've moved from understanding DORA through a vendor lens to building a 60-day action plan, integrating operational controls, preparing stakeholder playbooks, and embedding ongoing governance. That journey is practical, commercial, and achievable.

Immediate Actions

Convene your cross-functional squad, assign owners, and set the 60-day sprint start date within 72 hours

Build Momentum

Create gap register, define acceptance criteria, produce two interim evidence packages within three weeks

Sustain Progress

Establish governance cadence, automate evidence collection, embed resilience into product lifecycle

Go forward with confidence. Use these frameworks to reduce procurement friction, accelerate deal cycles, and build durable operational resilience. The next 60 days will be transformative for your vendor credibility with EU financial institutions.