GRCForce

Supplier Contract Audit Checklist for NIS2 and DORA

A practical checklist for reviewing critical supplier contracts against operational resilience, NIS2 and DORA expectations.

Published 15 June 2026 | GRCForce

Use this checklist to review whether your contracts with critical suppliers support real operational resilience, not just procurement completion.

This checklist is designed for organisations reviewing ICT, cloud, SaaS, managed service, and other material third-party relationships in scope for NIS2 andor DORA.

How to use this checklist

For each clause or question below, mark one of the following:

- ☐ In place and adequate
- ☐ Partially covered
- ☐ Missing
- ☐ Needs legal review

A contract does not need perfect wording on day one. It does need clear ownership of the gaps and a decision on whether the risk is acceptable.

12 contract clauses and questions to review

1. Right to audit

Does the contract give your organisation a practical right to obtain audit evidence, review control reports, and request follow-up where significant gaps are identified?

Why it matters: if you cannot test or review the supplier's controls in a credible way, you are relying on trust rather than assurance.

2. Security obligations

Are the supplier's baseline security obligations stated clearly, including protection of systems, access control, vulnerability management, logging, backup, recovery, and secure change management?

Why it matters: vague references to "industry standard security" are usually too weak when incidents occur.

3. Incident notification window

Does the contract define how quickly the supplier must notify you of a security incident, service disruption, data breach, or material control failure?

Why it matters: terms like "without undue delay" are often too loose for critical services. You need operationally useful timeframes.

4. Access and identity control

Does the contract define how privileged access is managed, how accounts are reviewed, and how access is revoked when personnel leave or when the service ends?

Why it matters: many supplier incidents start with weak administrative access and poor identity hygiene.

5. Data location and processing transparency

Can you identify where your data is processed, stored, backed up, and accessed from, including any use of subcontractors or overseas support teams?

Why it matters: resilience and regulatory exposure are harder to manage if data handling is opaque.

6. Subcontractor control

Does the supplier need your approval, or at least prior notification, before appointing material subcontractors that could affect service delivery, security, or compliance?

Why it matters: fourth-party risk often appears through hidden dependencies you never assessed.

7. Business continuity and disaster recovery

Does the contract require the supplier to maintain and test business continuity and disaster recovery arrangements appropriate to the criticality of the service?

Why it matters: resilience is not a statement. It needs recovery objectives, tested procedures, and evidence.

8. Service levels linked to criticality

Are service levels, recovery times, support commitments, and escalation paths aligned with the real business importance of the service?

Why it matters: many contracts are written as if the service were routine, even when it supports a critical process.

9. Data return, extraction, and deletion

Does the contract explain how your data will be returned, in what format, within what timeframe, at what cost, and how residual data will be deleted at exit?

Why it matters: if exit terms are unclear, you may be operationally locked in.

10. Change-of-control and material change clauses

Does the contract give you protection if the supplier is acquired, materially changes its service model, relocates operations, or changes key subcontractors?

Why it matters: supplier risk can change overnight without any change on your side.

11. Evidence and reporting obligations

Does the supplier have to provide regular evidence such as audit reports, test results, certifications, risk updates, or control attestations?

Why it matters: one-time due diligence is not enough for critical relationships.

12. Exit support and transition assistance

Does the contract require the supplier to support transition to another provider or to an internal service, including cooperation, documentation, and technical assistance?

Why it matters: resilience includes the ability to leave without severe disruption.

Red flags that deserve immediate attention

- ☐ No right to audit, or audit language that is purely discretionary
- ☐ No clear incident notification timeframe
- ☐ No clause covering subcontractor changes
- ☐ No tested recovery commitment for critical services
- ☐ No practical data extraction or deletion terms
- ☐ No exit support obligations
- ☐ No obligation to provide current assurance evidence
- ☐ No change-of-control protection

Quick scoring guide

- ☐ 10 to 12 items in place and adequate: strong contract baseline
- ☐ 7 to 9 items in place: workable, but review priority gaps

- ☐ 4 to 6 items in place: elevated contractual risk
- ☐ 0 to 3 items in place: contract should be considered high priority for remediation

Suggested use cases

This checklist works well for:

- ☐ Supplier onboarding reviews
- ☐ Contract renewal reviews
- ☐ DORA ICT third-party assessments
- ☐ NIS2 supplier risk reviews
- ☐ Procurement and legal alignment workshops
- ☐ Board or management reporting on third-party resilience

Official reference sources

These are useful official sources to include near the checklist, in the blog article, or in follow-up posts.

EU sources

- ☐ NIS2 Directive official text on EUR-Lex: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- ☐ DORA Regulation official text on EUR-Lex: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- ☐ European Commission finance page for DORA implementing and delegated acts: https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en
- ☐ ESMA overview page on DORA: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
- ☐ European Commission page on NIS2 implementation in Belgium: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-belgium

Belgian sources

- ☐ Centre for Cybersecurity Belgium NIS2 information portal: https://belgium-nis2.be/en/
- ☐ Centre for Cybersecurity Belgium main site: https://ccb.belgium.be/en
- ☐ CERT.be contact point via the European Commission Belgium implementation page: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-belgium

Short resource block for posts or article sidebars

Useful official sources if you are working through NIS2 or DORA:

- ☐ Official NIS2 text: EUR-Lex Directive (EU) 2022/2555
- ☐ Official DORA text: EUR-Lex Regulation (EU) 2022/2554
- ☐ DORA overview and updates: ESMA
- ☐ Belgium NIS2 implementation and contact points: European Commission Digital Strategy page
- ☐ Belgium practical NIS2 information: Centre for Cybersecurity Belgium

Suggested CTA for GRC Force

If you want a practical review of your top supplier contracts against this checklist, GRC Force helps organisations identify where legal wording, supplier governance, and operational resilience are out of sync.

Practical review support

Contact GRCForce to review where supplier contract wording, governance and operational resilience are out of sync: https://grcforce.com/en/#contact

This checklist is practical guidance and does not replace legal advice. Escalate contract wording and regulatory interpretation for appropriate legal review.