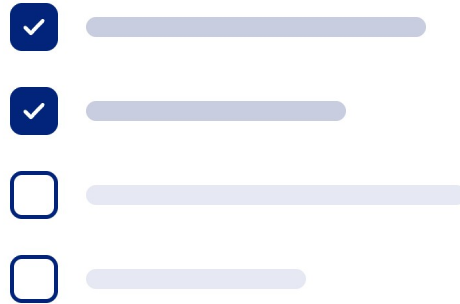




## CHECKLIST

# GRC implementation checklist

Avoid the challenges that stall your GRC implementation

This checklist follows the three levers that keep a GRC implementation moving: clear ownership, simpler processes and documentation you can maintain. Use it before you start, after 90 days and again at your annual review.

**1**

Clear ownership

**2**

Simpler processes

**3**

Documentation you can maintain

USE IT

Before you start

After 90 days

At your annual review

## 1 Before you start: obligations and mandate

- ☐ We've listed the laws and standards that apply to us (for example GDPR, NIS2, DORA, ISO 27001, the AI Act).
- ☐ We know which entities, systems and processes each obligation covers.
- ☐ If we're in NIS2 scope, we're registered with the competent authority.
- ☐ The management body has approved the programme, its scope and a reporting cadence.
- ☐ An executive sponsor has been appointed.
- ☐ A programme lead has been appointed, with time set aside for the role.
- ☐ We've assessed our maturity and agreed a target for year one.

## 2 Ownership

- ☐ We have a RACI matrix for the core activities.
- ☐ The management body approves risk measures and key policies (NIS2 Art. 20, DORA Art. 5).
- ☐ Every control has one named owner. A team or a shared inbox doesn't count.
- ☐ Every risk has one named risk owner.
- ☐ Every system, process and supplier has one named responsible person.
- ☐ Process owners keep their part of the GDPR Article 30 record up to date. The DPO advises and checks.
- ☐ Nobody independently checks their own work.
- ☐ Management body members have completed training, and it's documented.

### 3 Scope and first framework

- ☐ The first framework was chosen by legal obligation, not ambition.
- ☐ The pilot covers one business unit or a handful of critical systems.
- ☐ We'll take the pilot all the way to its first review before expanding.
- ☐ We've mapped which controls can be reused across frameworks.
- ☐ We've listed what can't be reused, such as NIS2 reporting deadlines, management training and DORA's register of information.
- ☐ The process was agreed before the tool was configured.
- ☐ We use standard templates and customise only where we genuinely differ.

### 4 Documentation you can maintain

- ☐ We keep only the documentation the rules require and the business needs.
- ☐ Every document has one named owner.
- ☐ Every document has a review date, set when it was created.
- ☐ Documents have version control and a change log (ISO 27001 clause 7.5.3).
- ☐ Evidence is stored with the control it proves, not in emails or personal drives.
- ☐ All recurring tasks sit in an annual wheel with an owner, a deadline and the expected evidence.
- ☐ There's a fixed date for retiring the old spreadsheet.

## 5 The first 90 days

### Days 0–30

- ☐ Mandate approved
- ☐ Obligations mapped
- ☐ Owners named

### Days 31–60

- ☐ First framework configured for the pilot area
- ☐ Minimum documentation under way
- ☐ Owners trained on their own tasks

### Days 61–90

- ☐ Spreadsheet retired
- ☐ First annual-wheel tasks completed
- ☐ First management report delivered

## 6 The annual wheel: ongoing operation



### Q1

- ☐ Review the record of processing
- ☐ Update the supplier list and classification

### Q2

- ☐ Update risk assessments
- ☐ Run an awareness campaign

### Q3

- ☐ Internal audit
- ☐ Test incident handling and continuity

### Q4

- ☐ Management review
- ☐ Approve risk measures, policies and next year's plan
- ☐ Management training

## 7 KPIs to track every quarter

- |                                                                                              |                                                                   |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| <input type="checkbox"/> Share of controls with a named owner (target: 100% after the pilot) | <input type="checkbox"/> Recurring tasks completed on time        |
| <input type="checkbox"/> Number of overdue risk treatment actions                            | <input type="checkbox"/> Evidence older than its review interval  |
| <input type="checkbox"/> Time to answer an auditor's evidence request                        | <input type="checkbox"/> Management reports delivered on schedule |
| <input type="checkbox"/> Management body training completed                                  | <input type="checkbox"/> Owners active in the platform            |

## 8 Warning signs: check them now

Tick any that apply.

- ☐ Tasks are assigned to "Compliance" or a shared inbox.
- ☐ Steering meetings are cancelled or postponed.
- ☐ More than two frameworks are in progress, but none is finished.
- ☐ The old spreadsheet is still being updated alongside the platform.
- ☐ We have evidence older than its review interval.
- ☐ Control owners rarely or never log in.
- ☐ Management hasn't received a GRC report this quarter.
- ☐ The DPO or CISO is the only person updating anything.

**Two or more ticks mean your implementation is starting to stall.**

Your ticks \_\_\_\_\_

# Want to see how this looks with your own frameworks?

.legal is a modular GRC platform that maps one task to controls across GDPR, NIS2, ISO 27001, DORA and the AI Act, with an annual wheel, named owners and management reporting.

GDPR

NIS2

ISO 27001

DORA

AI Act

## Book a demo

[dotlegal.com/en/product/get-a-demo/book-a-demo](https://dotlegal.com/en/product/get-a-demo/book-a-demo)

Book a demo →

## Read the full guide

[dotlegal.com/en/articles/compliance/grc-implementation](https://dotlegal.com/en/articles/compliance/grc-implementation)

Read the guide →