.legal



CHECKLIST

GRC software requirements checklist

Score vendors with a weighted scorecard and 14 questions to ask

Use this checklist when you compare GRC software on a shortlist. Agree the weights before the first demo, ask for a demonstration rather than a yes, and pilot with your own frameworks before you sign.

1
Weighted scorecard

2
14 questions to ask

3
Pilot before you sign

USE IT — In a demo · In a requirements document · In a tender

Published by .legal · dotlegal.com

8 pages

How to use it

1. **Agree the weights before the first demo.**
   Adjust them to your situation, but don't change them once you've seen the vendors.

2. **Ask for a demonstration rather than a yes.**
   Score only what you've seen working.

3. **Pilot with your own frameworks before you sign.**
   One of your frameworks, one of your real systems and one of your own control owners.

Scoring scale

SCORE	MEANING
1	Not supported
2	Possible only with workarounds or custom work
3	Supported, but only shown in a generic demo
4	Shown working in our scenario
5	Shown working with our own data or framework

A B C — A, B and C are the three vendors on your shortlist. Write each vendor's name on the line under its letter in the tables.

How to calculate: multiply each score by its weight and add the seven results for each vendor. The maximum is 5.0.

Score vendors with a weighted scorecard

Feature lists make every vendor look alike. A weighted scorecard forces you to test what matters to you and compare like with like.

Criterion	What to test in the demo or trial	Weight	Vendors · score 1–5 A	B	C
Ease of use for owners	Ask a control owner, not an administrator, to complete a task and upload evidence without help	**20%**			
Framework coverage and cross-mapping	Show one control mapped to ISO 27001, NIS2 and GDPR, and the same evidence counting in all three	**20%**			
Ownership, roles and access	Assign an owner at department level and show what a sign-off-only colleague sees	**15%**			
Recurring tasks and reporting	Create an annual-wheel task with reminders, then export a management report	**15%**			
Modularity and total cost	Price year one with your first framework, and year three with everything you expect to add	**10%**			
EU hosting, assurance and exit	Hosting location, ISAE 3402 or ISAE 3000 reports, and the format of a full data export	**10%**			
Onboarding, migration and support	Who imports your spreadsheets, how long it takes and what support response times look like	**10%**			
Weighted total (max 5.0)		**100%**			

Questions to ask in a demo or tender

Use these questions in a demo, a requirements document or a formal tender. Ask for a demonstration rather than a yes.

#	Question	Vendors Shown in the demo? (Yes / Partly / No) A Y	A P	A N	B Y	B P	B N	C Y	C P	C N	Notes
	FRAMEWORKS										
1	Which frameworks are included out of the box, and how do you keep them up to date when rules change?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2	Can one task or control count towards several frameworks, and can you show it?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
	OWNERSHIP AND ACCESS										
3	How do we assign a single named owner to an asset, process, supplier or control?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
4	Can access be limited by role and by department or group company?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
5	How do colleagues who aren't platform users receive and sign off policies?	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Questions to ask in a demo or tender, continued

#	Question	Vendors Shown in the demo? (Yes / Partly / No) A Y	A P	A N	B Y	B P	B N	C Y	C P	C N	Notes
	OPERATIONS AND REPORTING										
6	How are recurring tasks scheduled, assigned and followed up?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
7	What does a management report look like, and can it be exported without a login?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
8	How do risk assessments link to the assets and processes we've already mapped?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
9	What audit trail and version history do you keep for documents and decisions?	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Questions to ask in a demo or tender, continued

#	Question	Vendors Shown in the demo? (Yes / Partly / No) A Y	A P	A N	B Y	B P	B N	C Y	C P	C N	Notes
	HOSTING, ASSURANCE AND EXIT										
10	Where is our data hosted, and which sub-processors do you use?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
11	Which assurance reports can you share, such as ISAE 3402, ISAE 3000 or ISO 27001?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
12	How do we get all our data out if we leave, and in which format?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
	ONBOARDING AND COST										
13	Who handles migration from our spreadsheets, and what does onboarding include?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
14	What will year three cost if we add two more modules or frameworks?	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Pilot with your own frameworks before you sign

A generic demo shows the vendor at its best. Ask to see the platform with one of your own frameworks, one of your real systems and one of your own control owners. If the vendor can't do that before you sign, expect the same after.

	A	B	C
One of our own frameworks	☐	☐	☐
One of our real systems	☐	☐	☐
One of our own control owners completed a task without help	☐	☐	☐

! Warning signs before you sign

Tick any that apply.

- ☐ We haven't decided who owns what yet.
- ☐ A control owner couldn't complete a task in the demo without help.
- ☐ We've only seen a generic demo, not our own frameworks or systems.
- ☐ We don't know the price for year three.
- ☐ The vendor can't show the format of a full data export.

Two or more ticks: pause the purchase and close the gaps first.

Your ticks _____

Planning the rollout too?

.legal

Most GRC projects stall after the contract is signed, for organisational reasons. Plan ownership, scope and documentation before go-live.

Book a demo

dotlegal.com/en/product/get-a-demo/book-a-demo

Book a demo →

Read the GRC software guide

dotlegal.com/en/articles/compliance/grc-software

Read the guide →

Get the GRC implementation checklist

dotlegal.com/en/articles/compliance/grc-implementation

Get the checklist →

This checklist is for guidance and doesn't replace legal or procurement advice. Published by .legal · dotlegal.com