.legal



TJEKLISTE

Kravspecifikation til GRC-software

Sammenlign leverandører med et vægtet scorecard og 14 spørgsmål

Brug tjeklisten, når I sammenligner GRC-software på en kortliste. Aftal vægtene før første demo, bed om at få tingene vist frem for et ja, og afprøv med jeres egne frameworks, før I skriver under.

1
Vægtet scorecard

2
14 spørgsmål til leverandøren

3
Afprøv før I skriver under

BRUG DEN

- Til demo
- I en kravspecifikation
- I et udbud

Udgivet af .legal · dotlegal.com

Sådan bruger I den

1. **Aftal vægtene før første demo.**
   Juster dem til jeres situation, men ændr dem ikke, når I har set leverandørerne.

2. **Bed om at få det vist frem for et ja.**
   Giv kun point for det, I har set virke.

3. **Afprøv med jeres egne frameworks, før I skriver under.**
   Et af jeres frameworks, et af jeres rigtige systemer og en af jeres egne kontrolejere.

Pointskala

POINT	BETYDNING
1	Understøttes ikke
2	Kun muligt med workarounds eller tilkøbt udvikling
3	Understøttes, men kun vist i en generisk demo
4	Vist i vores scenarie
5	Vist med vores egne data eller vores eget framework

A B C — A, B og C er de tre leverandører på jeres kortliste. Skriv leverandørens navn på stregen under bogstavet i tabellerne.

Sådan regner I: gang hvert point med vægten, og læg de syv resultater sammen for hver leverandør. Maksimum er 5,0.

Sammenlign leverandører med et vægtet scorecard

Funktionslister får alle leverandører til at ligne hinanden. Et vægtet scorecard tvinger jer til at teste det, der betyder noget for jer, og sammenligne på samme grundlag.

Kriterie	Det skal I teste i demo eller prøveperiode	Vægt	Leverandører · point 1-5 A	B	C
Brugervenlighed for ejerne	Lad en kontrolejer, ikke en administrator, løse en opgave og uploade dokumentation uden hjælp	**20 %**	☐	☐	☐
Frameworks og mapping på tværs	Vis én kontrol koblet til ISO 27001, NIS2 og GDPR, og den samme dokumentation, der tæller i alle tre	**20 %**	☐	☐	☐
Ejerskab, roller og adgang	Tildel en ejer på afdelingsniveau, og vis hvad en kollega, der kun skal kvittere, ser	**15 %**	☐	☐	☐
Tilbagevendende opgaver og rapportering	Opret en opgave i årshjulet med påmindelser, og eksporter en ledelsesrapport	**15 %**	☐	☐	☐
Modulopbygning og samlet pris	Pris for år ét med første framework og for år tre med alt det, I forventer at tilføje	**10 %**	☐	☐	☐
Hosting i EU, erklæringer og exit	Hostingsted, ISAE 3402- eller ISAE 3000-erklæringer og formatet på et fuldt dataudtræk	**10 %**	☐	☐	☐
Onboarding, migrering og support	Hvem importerer jeres regneark, hvor lang tid tager det, og hvordan er svartiderne i support	**10 %**	☐	☐	☐
Vægtet total (maks. 5,0)		**100 %**	☐	☐	☐

Spørgsmål til demo eller udbud

Brug spørgsmålene til en demo, en kravspecifikation eller et formelt udbud. Bed om at få det vist frem for et ja.

		Leverandører Vist i demo? (Ja / Delvist / Nej)									
		A			B			C			
#	Spørgsmål	J	D	N	J	D	N	J	D	N	Noter
	FRAMEWORKS										
1	Hvilke frameworks følger med, og hvordan holder I dem opdateret, når reglerne ændrer sig?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2	Kan én opgave eller kontrol tælle i flere frameworks, og kan I vise det?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
	EJERSKAB OG ADGANG										
3	Hvordan giver vi et aktiv, en proces, en leverandør eller en kontrol én navngiven ejer?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
4	Kan adgangen begrænses efter rolle og efter afdeling eller koncernselskab?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
5	Hvordan modtager og kvitterer kolleger, der ikke er brugere af platformen, for politikker?	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Spørgsmål til demo eller udbud, fortsat

#	Spørgsmål	Leverandører – Vist i demo? (Ja / Delvist / Nej) A J	A D	A N	B J	B D	B N	C J	C D	C N	Noter
	DRIFT OG RAPPORTERING										
6	Hvordan planlægges, fordeles og følges der op på tilbagevendende opgaver?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
7	Hvordan ser en ledelsesrapport ud, og kan den eksporteres uden login?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
8	Hvordan kobles risikovurderinger til de aktiver og processer, vi allerede har kortlagt?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
9	Hvilken audit trail og versionshistorik gemmer I for dokumenter og beslutninger?	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Spørgsmål til demo eller udbud, fortsat

#	Spørgsmål	Leverandører – Vist i demo? (Ja / Delvist / Nej) A J	A D	A N	B J	B D	B N	C J	C D	C N	Noter
HOSTING, ERKLÆRINGER OG EXIT											
10	Hvor hostes vores data, og hvilke underdatabehandlere bruger I?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
11	Hvilke erklæringer kan I dele, fx ISAE 3402, ISAE 3000 eller ISO 27001?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
12	Hvordan får vi alle vores data ud, hvis vi skifter, og i hvilket format?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
ONBOARDING OG PRIS											
13	Hvem står for migrering fra vores regneark, og hvad indeholder onboardingen?	☐	☐	☐	☐	☐	☐	☐	☐	☐	
14	Hvad koster år tre, hvis vi tilføjer to moduler eller frameworks mere?	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Afprøv med jeres egne frameworks, før I skriver under

En generisk demo viser leverandøren fra den bedste side. Bed om at se platformen med et af jeres egne frameworks, et af jeres rigtige systemer og en af jeres egne kontrolejere. Kan leverandøren ikke det, før I skriver under, så forvent det samme bagefter.

	A	B	C
Et af vores egne frameworks	☐	☐	☐
Et af vores rigtige systemer	☐	☐	☐
En af vores egne kontrolejere løste en opgave uden hjælp	☐	☐	☐

! Advarselstegn før I skriver under

Sæt kryds, hvis det passer på jer.

- ☐ Vi har endnu ikke besluttet, hvem der ejer hvad.
- ☐ En kontrolejer kunne ikke løse en opgave i demoen uden hjælp.
- ☐ Vi har kun set en generisk demo, ikke vores egne frameworks eller systemer.
- ☐ Vi kender ikke prisen for år tre.
- ☐ Leverandøren kan ikke vise formatet på et fuldt dataudtræk.

To kryds eller flere: sæt købet på pause, og luk hullerne først.

Antal kryds _____

Skal I også planlægge udrulningen?

.legal

De fleste GRC-projekter går i stå, efter kontrakten er underskrevet, af organisatoriske grunde. Planlæg ejerskab, scope og dokumentation før go-live.

Book en demo

dotlegal.com/da/produkt/demo/book-en-demo

Book en demo →

Læs guiden til GRC-software

dotlegal.com/da/artikler/compliance/grc-software

Til guiden →

Hent tjeklisten til GRC-implementering

dotlegal.com/da/artikler/compliance/grc-implementering

Hent tjeklisten →