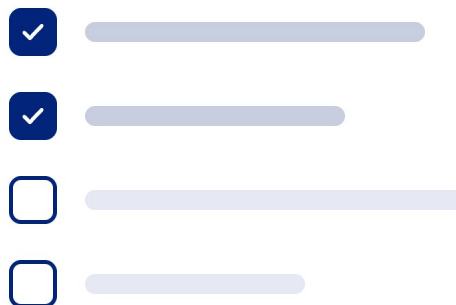




TJEKLISTE

GRC-implementering: tjekliste

Undgå det, der får jeres GRC-implementering til at gå i stå

Tjeklisten følger de tre greb, der holder en GRC-implementering i gang: klart ejerskab, enklere processer og dokumentation, der kan vedligeholdes. Brug den før I starter, efter 90 dage og igen ved den årlige gennemgang.

1

Klart ejerskab

2

Enklere processer

3

Dokumentation, der kan vedligeholdes

BRUG DEN

Før I starter

Efter 90 dage

Ved den årlige gennemgang

1 Før I starter: forpligtelser og mandat

- ☐ Vi har listet de love og standarder, der gælder for os (fx GDPR, NIS2, DORA, ISO 27001, AI-forordningen).
- ☐ Vi ved, hvilke selskaber, systemer og processer hver forpligtelse dækker.
- ☐ Er vi omfattet af NIS2, er vi registreret hos den kompetente myndighed.
- ☐ Ledelsesorganet har godkendt programmet, dets scope og en rapporteringsrytme.
- ☐ Der er udpeget en sponsor i direktionen.
- ☐ Der er udpeget en programleder med tid afsat til opgaven.
- ☐ Vi har vurderet vores modenhed og aftalt et mål for første år.

2 Ejerskab

- ☐ Vi har en RACI-matrix for de centrale aktiviteter.
- ☐ Ledelsesorganet godkender risikoforanstaltninger og centrale politikker (NIS2 art. 20, DORA art. 5).
- ☐ Hver kontrol har én navngiven ejer. Et team eller en fælles postkasse tæller ikke.
- ☐ Hver risiko har én navngiven risikoejer.
- ☐ Hvert system, hver proces og leverandør har én navngiven ansvarlig.
- ☐ Procesejerne holder deres del af fortegnelsen (GDPR art. 30) opdateret. DPO'en rådgiver og kontrollerer.
- ☐ Ingen kontrollerer uafhængigt deres eget arbejde.
- ☐ Ledelsesorganets medlemmer har fået undervisning, og det er dokumenteret.

3 Scope og første framework

- ☐ Første framework er valgt ud fra lovpligt, ikke ambition.
- ☐ Piloten dækker én forretningsenhed eller en håndfuld kritiske systemer.
- ☐ Vi tager piloten helt igennem til første gennemgang, før vi udvider.
- ☐ Vi har kortlagt, hvilke kontroller kan genbruges på tværs af frameworks.
- ☐ Vi har listet det, der ikke kan genbruges, fx NIS2-indberetningsfrister, ledelsens undervisning og DORA's informationsregister.
- ☐ Processen er aftalt, før værktøjet sættes op.
- ☐ Vi bruger standardskabeloner og tilpasser kun, hvor vi reelt er anderledes.

4 Dokumentation, der kan vedligeholdes

- ☐ Vi har kun den dokumentation, reglerne kræver, og forretningen har brug for.
- ☐ Hvert dokument har én navngiven ejer.
- ☐ Hvert dokument har en revisionsdato, der blev sat ved oprettelsen.
- ☐ Dokumenter har versionsstyring og ændringslog (ISO 27001 punkt 7.5.3).
- ☐ Dokumentation gemmes ved den kontrol, den beviser, ikke i mails eller på personlige drev.
- ☐ Alle tilbagevendende opgaver ligger i et årshjul med ejer, frist og forventet dokumentation.
- ☐ Der er en fast dato for at udfase det gamle regneark.

5 De første 90 dage

Dag 0-30

- ☐ Mandat godkendt
- ☐ Forpligtelser kortlagt
- ☐ Ejere navngivet

Dag 31-60

- ☐ Første framework sat op for pilotområdet
- ☐ Minimumsdokumentation i gang
- ☐ Ejerne er trænet i deres egne opgaver

Dag 61-90

- ☐ Regnearket er udfaset
- ☐ De første opgaver i årshjulet er gennemført
- ☐ Første ledelsesrapport er leveret

6 Årshjulet: løbende drift



K1

- ☐ Gennemgå fortegnelsen
- ☐ Opdater leverandørliste og klassificering

K2

- ☐ Opdater risikovurderinger
- ☐ Gennemfør awareness-kampagne

K3

- ☐ Intern audit
- ☐ Test hændelseshåndtering og beredskab

K4

- ☐ Ledelsens evaluering
- ☐ Godkend foranstaltninger, politikker og næste års plan
- ☐ Ledelsesundervisning

7 Nøgletal at følge hvert kvartal

- | | |
|---|---|
| ☐ Andel kontroller med navngiven ejer (mål: 100 % efter piloten) | ☐ Tilbagevendende opgaver løst til tiden |
| ☐ Antal forsinkede risikohåndteringstiltag | ☐ Dokumentation ældre end revisionsintervallet |
| ☐ Tid til at besvare en auditors forespørgsel | ☐ Ledelsesrapporter leveret til tiden |
| ☐ Ledelsens undervisning gennemført | ☐ Ejere, der er aktive i platformen |

8 Advarselstegn: tjek dem nu

Sæt kryds, hvis det passer på jer.

- ☐ Opgaver er tildelt "Compliance" eller en fælles indbakke.
- ☐ Styregruppemøder bliver aflyst eller udskudt.
- ☐ Mere end to frameworks er i gang, men intet er færdigt.
- ☐ Det gamle regneark opdateres stadig ved siden af.
- ☐ Vi har dokumentation, der er ældre end dens revisionsinterval.
- ☐ Kontroljere logger sjældent eller aldrig ind.
- ☐ Ledelsen har ikke modtaget en GRC-rapport i dette kvartal.
- ☐ DPO'en eller CISO'en er den eneste, der opdaterer noget.

To kryds eller flere betyder, at implementeringen er ved at gå i stå.

Antal kryds _____

Vil I se, hvordan det ser ud med jeres egne frameworks?

.legal er en modulopbygget GRC-plattform, der kobler én opgave til kontroller i GDPR, NIS2, ISO 27001, DORA og AI-forordningen, med årshjul, navngivne ejere og ledelsesrapportering.

GDPR

NIS2

ISO 27001

DORA

AI-forordningen

Book en demo

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

Book en demo →

Læs hele guiden

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

Til guiden →