# Leverandørstyringsmodel

Template: Leverandørstyringsmodel for Robot-, Drone- og Automationsindustrien udarbejdet udfra ISO27001 standardens kravelementer og forslag til aktionspunkter.

## Indhold



## Formål og anvendelse

Formålet med denne leverandørstyringsmodel er at sikre en effektiv styring af informationssikkerhedsrisici i forsyningskæden for robot-, drone- og automationsindustrien. Modellen er udviklet til undervisningsbrug og skal ses som inspiration til emnet leverandørstyring.

Modellen tager udgangspunkt i ISO27001 standardens kravelementer, men er ikke en komplet liste, der garanterer en korrekt anvendelse af ISO-standarden. Den enkelte virksomhed opfordres til at erhverve sig ISO 27001 standarden hos Dansk Standard samt uddanne sit eget personale i anvendelse af standarden. Hos Dubex kan vi bidrage til dette med uddannelse, rådgivning og vejledning.

Hos Dubex har vi udviklet ydelsen Security Maturity Assessment, der giver virksomhedens ledelse et overblik over det aktuelle modenhedsniveau baseret på en

generel gennemgang af de tekniske, fysiske og organisatoriske sikkerhedsforhold set i forhold til standardrammeværker som fx ISO27001.

# Introduktion til Leverandørstyringsmodeller

En leverandørstyringsmodel udgøres af en kompleks sammensætning af diverse komponenter. Disse komponenter omfatter, men er ikke begrænset til:

- Kontinuerlige impact assesments og risikovurderinger
- Kontraktuelle forpligtelser
- Sikkerhedsrevisioner
- Leverandørens egenkontrol og indrapportering
- Flerniveaukommunikation
- Sikre kanaler til informationsudveksling
- Inddragelse i beredskab fx ifm. NIS2, CER eller CRA
- Exitstrategier og procedurer for leverandørskifte

Grundet denne models omfattende og mangefacetterede natur er det essentielt at allokere tilstrækkelige ressourcer til styring og overvågning af leverandørkæder.

I det følgende præsenteres en sammenfatning af emner og elementer, som den enkelte virksomhed bør tage i betragtning ved udformningen og implementeringen af forsynings- og leverandørkædestrategier. Emnerne er opstillet i en logisk rækkefølge, der afspejler en typisk implementeringsproces, og kan således integreres i virksomhedens strategi i den angivne sekvens.

Berig gerne modellen med egne betragtninger og emner til afklaring af leverandørforhold.

## 0. Leverandørstyringsprocessen

### *0.1 Opsætning af politikker og årshjul*

- Leverandørstyringspolitik med tilhørende ansvarsplacering i organisationen
- Formaliseret årshjul for at sikre en årlig periodisk vurdering og håndtering af informationssikkerheds risici i relation til leverandører i forsyningskæden
- Procedure for ledelses godkendelse årligt eller ved ændringer i processen.

## 1. Risikovurdering af leverandører

### *1.1 Indledende risikovurdering*

- Kortlæg implicerede systemer og leverandører i forsyningskæden

- Kategorisér leverandører baseret på kritikalitet og adgang til sensitive data/systemer
- Vurdér leverandørens cybersikkerheds- og modenhedsniveau
- Identificér potentielle sårbarheder i leverandørens produkter eller tjenester

### *1.2 Løbende risikovurdering*

- Implementér en proces for regelmæssig genvurdering af leverandørrisici
- Overvåg ændringer i leverandørens forretning eller sikkerhedsstatus

## 2. Kontraktuelle krav

### *2.1 Sikkerhedskrav*

- Definer specifikke sikkerhedskrav baseret på risikovurderingen
- Definer sikkerhedskrav til underleverandører i forsyningskæden
- Inkludér krav om overholdelse af relevante standarder, love og regulativer

### *2.2 Audit og overvågning*

- Fastlæg ret til at udføre sikkerhedsaudits; virtuel, fysisk og/eller via 3. part partner
- Definer krav til leverandørens egen sikkerhedsovervågning og rapportering

### *2.3 Incident response*

- Specificér krav til leverandørens håndtering og rapportering af sikkerhedshændelser
- Definer eskaleringsprocesser og kommunikationskanaler

## 3. Leverandørevaluering og -godkendelse

### *3.1 Due diligence*

- Udfør baggrundstjek og finansiel vurdering
- Evaluér leverandørens egen cybersikkerhedspraksis og certificeringer
- Evaluér leverandørens underleverandørkæde og afhængigheder

### *3.2 Godkendelsesproces*

- Implementér en formel godkendelsesproces for nye leverandører
- Definer kriterier for godkendelse baseret på sikkerhedskrav og risikoniveau

## 4. Løbende leverandørstyring

### *4.1 Performance-overvågning*

- Etablér KPI'er for leverandørens sikkerhedsperformance

- Implementér regelmæssig rapportering og evaluering

### *4.2 Sikkerhedsopdateringer og patch management*

- Definer proces for håndtering af sikkerhedsopdateringer i leverandørprodukter
- Implementér krav om rettidig installation af kritiske patches

### *4.3 Adgangsstyring*

- Implementér princippet om mindst mulig adgang for leverandører
- Regelmæssig gennemgang og opdatering af leverandøradgang

## 5. Sikker informationsdeling

### *5.1 Datadeling og -klassificering*

- Definer retningslinjer for klassificering af data, der deles med leverandører/underleverandører
- Implementér sikre kanaler for informationsdeling

### *5.2 Fortrolighedsaftaler*

- Udarbejd og håndhæv omfattende fortrolighedsaftaler med alle leverandører

## 6. Leverandøruddannelse og -bevidsthed

### *6.1 Sikkerhedstræning*

- Tilbyd eller kræv regelmæssig sikkerhedstræning for leverandørpersonale
- Fokusér på branchespecifikke trusler og best practices

### *6.2 Awareness-programmer*

- Implementér programmer for at øge bevidstheden om cybersikkerhed hos leverandører
- Del relevante trusselsefterretninger og sikkerhedsopdateringer

## 7. Beredskabsplanlægning og kontinuitet

### *7.1 Beredskabsplaner*

- Kræv, at leverandører har dokumenterede beredskabsplaner
- Inkludér leverandører i organisationens egne beredskabsøvelser

### *7.2 Forsyningskædekontinuitet*

- Udvikl strategier for at håndtere leverandørsvigt eller -kompromittering
- Identificér alternative leverandører for kritiske komponenter eller tjenester

## 8. Afslutning af leverandørforhold

### *8.1 Exit-strategi*

- Definer proces for sikker afslutning af leverandørforhold
- Sikr tilbagelevering eller sikker destruktion af data og aktiver

### *8.2 Overgangsplanlægning*

- Planlæg for sikker overgang til nye leverandører eller intern håndtering

## 9. Dokumentation og revision

### *9.1 Dokumentationskrav*

- Opretholdt detaljeret dokumentation af alle leverandørinteraktioner og -vurderinger
- Implementér et system til styring af leverandørdokumentation

### *9.2 Regelmæssig revision*

- Udfør regelmæssige interne revisioner af leverandørstyringsprocessen
- Tilpas modellen baseret på revisionsresultater og ændrede trusselsbilleder

# Dubex

"Vi er stadig drevet af ønsket om at skabe de bedst mulige sikkerhedsløsninger til vores kunder." - Gorm Mandsberg, Dubex CEO

Dubex blev grundlagt i 1997 af Gorm Mandsberg, Klaus Kongsted og Jacob Herbst og fejrer sit 25-års jubilæum i 2022. Helt fra begyndelsen har vi arbejdet med cyber- og informationssikkerhed og relaterede teknologier. I de første år var en stor del af jobbet at uddanne markedet og forklare vigtigheden af it-sikkerhed og ikke mindst, hvad de forskellige sikkerhedsprodukter egentlig var, og hvad de var gode til.

I de senere år er der med den altomfattende digitalisering kommet mere fokus på vigtigheden af cyber- og informationssikkerhed, som er blevet forretningskritisk. Som følge heraf blev rådgivning en vigtigere del af Dubex' arbejde, og hjælp til at udarbejde og implementere politikker og styring blev en væsentlig del af vores arbejde.

Se mere på www.dubex.dk