Enligne
Regie op IT, data en projecten

Checklist IT- & datarisico's

Strategie & governance

- Is er een actuele IT- en datastrategie die expliciet is afgestemd met de directie?
- Zijn rollen en verantwoordelijkheden voor IT-beslissingen duidelijk belegd (directie, IT, externe partijen)?
- Is er een aangewezen eigenaar voor IT- en datarisico's binnen het MT?
- Worden grote IT- en dataprojecten altijd vooraf getoetst op risico, impact en businesscase?

Kritieke processen & systemen

- Zijn de belangrijkste bedrijfsprocessen en de bijbehorende systemen volledig in kaart gebracht?
- Is duidelijk welke systemen "bedrijfskritiek" zijn (uitval = stilstand of grote schade)?
- Is er een actueel overzicht van alle koppelingen tussen systemen (intern en extern)?
- Is bekend welke processen afhankelijk zijn van één persoon of één leverancier?

Data & privacy

- Weet u waar uw belangrijkste data staat (locatie, leverancier, land/jurisdictie)?
- Is vastgelegd wie toegang heeft tot welke data (rollen, rechten, functies)?
- Worden back-ups niet alleen gemaakt, maar ook periodiek getest op herstel?
- Zijn privacy- en dataklasseringen (bijv. vertrouwelijk, strikt vertrouwelijk) vastgelegd en bekend?

Beveiliging & toegang

- Is multi-factor authenticatie standaard voor kritieke systemen en accounts?
- Worden gebruikersrechten periodiek opgeschoond (ex-medewerkers, rolwijzigingen)?
- Zijn er duidelijke procedures voor het melden en afhandelen van beveiligingsincidenten en datalekken?
- Worden logins, verdachte activiteiten en mislukte inlogpogingen actief gemonitord?

Leveranciers & contracten

- Zijn de belangrijkste IT-leveranciers en hun onderlinge afhankelijkheden in kaart gebracht?
- Staan beschikbaarheid, responstijden, beveiliging en datalocatie expliciet in contracten/SLA's?
- Is er een exit-strategie als een leverancier uitvalt of niet levert (data, continuïteit, kennis)?
- Worden leveranciers periodiek geëvalueerd op prestaties én risico's?

Continuïteit & herstel

- Bestaat er een getest noodplan bij uitval van systemen, ransomware of dataverlies?

- Is bekend hoe lang het bedrijf kan doordraaien bij IT-storingen (RTO/RPO)?
- Zijn scenario's als ransomware, langdurige cloud-uitval en verlies van kritieke data uitgewerkt?
- Zijn verantwoordelijkheden en communicatielijnen in crisissituaties vooraf vastgelegd?

Mens & gedrag

- Krijgen medewerkers regelmatig training of bewustwordingssessies over IT- en datarisico's?
- Zijn er duidelijke richtlijnen voor gebruik van eigen devices, cloudoplossingen en schaduw-IT?
- Worden incidenten zonder schuldvraag geëvalueerd om ervan te leren?
- Is er aandacht voor gedrag en cultuur rondom "veilig werken met data"?