Integrity360
your security in mind

Cyber Risk & Assurance (CRA) Checklista

Är du redo för ett verkligt hot?

Använd denna checklista för att utvärdera din organisations beredskap, identifiera cyberrisk-blinda fläckar och ta proaktiva steg mot digital motståndskraft. Integrity360 hjälper organisationer att identifiera luckor, bedöma hot och anpassa sig till viktiga regelverk som DORA, NIS2 och ISO 27001. Du bör ställa dig följande frågor:

1. Styrning & Riskhantering

- [ ] Har vi en dokumenterad cyberriskstrategi som är anpassad till affärsmålen?
- [ ] Bedöms, prioriteras och ägs cyberrisker formellt?
- [ ] Har vi kartlagt våra kritiska affärstillgångar och tjänster?
- [ ] Granskar och uppdaterar vi regelbundet vårt riskregister?

2. Tekniska kontroller & Synlighet

- [ ] Har vi insyn i alla endpoints, nätverk och molninfrastruktur?
- [ ] Är våra kritiska tillgångar skyddade med lagerbaserad säkerhet (t.ex. EDR, brandväggar, segmentering)?
- [ ] Är vårt sårbarhetshanteringsprogram effektivt och kontinuerligt?
- [ ] Övervakar vi avvikelser eller tidiga kompromissindikatorer?

3. Detektion & Responsförmåga

- [ ] Har vi en definierad och testad incident-responsplan?
- [ ] Prioriteras larm baserat på risk och affärspåverkan?
- [ ] Har vi verktyg för att upptäcka och undersöka misstänkt aktivitet i realtid?
- [ ] Kan vi begränsa och återhämta oss från ransomware inom timmar, inte dagar?

4. Människor, Processer & Medvetenhet

- [ ] Är personalen utbildad i att känna igen phishing, social engineering och insiderhot?
- [ ] Finns det formella processer för åtkomst-kontroll, onboarding och offboarding?
- [ ] Har vi testat teamets respons genom tabletop- eller red team-övningar?
- [ ] Har vi definierade roller och ansvar för cyber security?

5. Tredjeparts- & Leverantörsrisker

- [ ] Bedömer vi våra nyckelleverantörers cyber security-nivå?
- [ ] Granskas och riskbedöms tredjeparts datadelningsavtal regelbundet??
- [ ] Övervakas och kontrolleras tredjepartsåtkomst på ett korrekt sätt?

Hur gick det?

Om något av ovanstående saknas är det dags för en omfattande bedömning av cybersäkerhets-mognaden för att hjälpa dig att utvärdera, anpassa och förbättra din säkerhetsstatus.

Låt oss hjälpa dig att upptäcka risker och bygga upp motståndskraft.

Jag är redo för en djupgående bedömning av cybersäkerhetsmognad