

Checklist

5.8 – Informatiebeveiliging in projectbeheer

Thema: Organisatorisch | ISO 27002: 5.8 | Gerelateerd: 5.1, 8.25

Doelstelling

Aantonen dat informatiebeveiliging structureel wordt meegenomen in projecten, van initiatie tot oplevering, zodat beveiligingsrisico's tijdig worden geïdentificeerd en beheerst.

Beleid en kaders

- ☐ Is er beleid dat informatiebeveiliging verplicht meeneemt in projectbeheer?
- ☐ Is de beveiligingsfunctionaris (CISO of vertegenwoordiger) betrokken bij alle relevante projecten?
- ☐ Zijn beveiligingseisen opgenomen in de projectmethodologie (Prince2, Agile, etc.)?
- ☐ Worden beveiligingseisen al in de initiatiefase van een project gedefinieerd?

Risicoanalyse in projecten

- ☐ Wordt een Privacy Impact Assessment (DPIA) uitgevoerd bij projecten met persoonsgegevens?
- ☐ Wordt een beveiligingsrisicoanalyse uitgevoerd voor projecten met nieuwe systemen of processen?
- ☐ Worden beveiligingsrisico's opgenomen in het projectrisicoregister?
- ☐ Is er een go/no-go moment voor beveiliging vóór livegang van een nieuw systeem?
- ☐ Worden beveiligingseisen meegenomen in acceptatietesten vóór oplevering?

Beveiliging in ontwerp en ontwikkeling

- ☐ Worden beveiligingseisen (security by design) opgenomen in de functionele en technische specificaties?
- ☐ Is privacy by design toegepast bij projecten met verwerking van persoonsgegevens?
- ☐ Worden beveiligingsreviews (code review, architectuurreview) uitgevoerd tijdens ontwikkeling?
- ☐ Is er een Secure Software Development Lifecycle (SSDLC) of vergelijkbaar proces?

Oplevering en overdracht

- ☐ Is beveiliging een formeel opleveringscriterium voor projecten?
- ☐ Worden beveiligingsdocumentatie en -configuraties overgedragen aan de beheerorganisatie?
- ☐ Is vastgelegd wie na oplevering verantwoordelijk is voor de beveiliging van het systeem?



Worden lessen op beveiligingsgebied na afronding van een project vastgelegd en gedeeld?

Verantwoordelijke:	_____	Datum controle:	_____
Afdeling:	_____	Score:	___ / 21
Reviewcyclus:	☐ Jaarlijks ☐ Na wijziging ☐ Na incident		Status: ☐ Voldoet ☐ Actiepunt ☐ N.v.t.