

Checklist

8.30 – Uitbestede ontwikkeling

Thema: Technisch | ISO 27002: 8.30 | Gerelateerd: 8.25, 5.19

Doelstelling

Aantonen dat uitbestede softwareontwikkeling voldoet aan de beveiligingseisen van de organisatie en dat de kwaliteit en veiligheid van het opgeleverde werk worden gecontroleerd.

Contractuele beveiligingseisen

- ☐ Zijn beveiligingseisen voor softwareontwikkeling opgenomen in contracten met externe partijen?
- ☐ Is de eis voor naleving van secure coding guidelines contractueel vastgelegd?
- ☐ Zijn vereisten voor beveiligingstesten en -rapportage opgenomen in het contract?
- ☐ Is het recht op inspectie en audit van het ontwikkelproces contractueel verankerd?
- ☐ Is vastgelegd hoe de externe partij omgaat met kwetsbaarheden na oplevering?

Kwaliteits- en beveiligingscontrole

- ☐ Wordt opgeleverde code beoordeeld op beveiliging vóór acceptatie?
- ☐ Worden beveiligingstesten uitgevoerd op door externe partijen opgeleverde software?
- ☐ Wordt de externe partij beoordeeld op hun secure development volwassenheid?
- ☐ Zijn audittrails en documentatie van het ontwikkelproces beschikbaar?

Toegang en intellectueel eigendom

- ☐ Is toegang van externe ontwikkelaars tot interne systemen en data beperkt tot het noodzakelijke?
- ☐ Worden externe ontwikkelaars gescreend conform het screeningsbeleid?
- ☐ Is het eigendom van de ontwikkelde software contractueel vastgelegd bij de organisatie?
- ☐ Worden NDA's afgesloten met externe ontwikkelaars die toegang hebben tot vertrouwelijke informatie?

Overdracht en nazorg

- ☐ Is broncode aantoonbaar overgedragen bij oplevering?
- ☐ Is documentatie (technisch, functioneel, beveiligingsarchitectuur) meegeleverd?
- ☐ Zijn afspraken gemaakt over ondersteuning en patching na oplevering?



Worden kwetsbaarheden ontdekt na oplevering gemeld aan en opgepakt door de externe partij?

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