

Checklist

8.34 – Bescherming van informatiesystemen tijdens audittesten

Thema: Technisch | ISO 27002: 8.34 | Gerelateerd: 8.29, 5.35

Doelstelling

Aantonen dat audittesten en beveiligingsbeoordelingen van productiesystemen worden gepland en uitgevoerd op een manier die de beschikbaarheid en integriteit van systemen niet in gevaar brengt.

Planning van audittesten

- ☐ Worden audittesten en beveiligingsscan van productiesystemen vooraf gepland en goedgekeurd?
- ☐ Is het change management proces gevolgd voor het uitvoeren van audittesten in productie?
- ☐ Is de scope en impact van audittesten vooraf beoordeeld?
- ☐ Worden audittesten bij voorkeur buiten kantooruren of piekbelasting uitgevoerd?
- ☐ Zijn systeemeigenaren tijdig geïnformeerd over geplande audittesten?

Toegang en autorisatie voor auditors

- ☐ Is toegang van auditors tot productiesystemen beperkt tot het strikt noodzakelijke?
- ☐ Worden aparte, tijdelijke accounts aangemaakt voor auditors?
- ☐ Worden auditaccounts direct geblokkeerd na afloop van de audit?
- ☐ Worden handelingen van auditors gelogd gedurende de gehele audittestperiode?

Uitvoering van audittesten

- ☐ Worden destructieve of verstorende tests alleen uitgevoerd in testomgevingen?
- ☐ Is er een rollback- of herstelplan beschikbaar bij onverwachte verstoring door audittesten?
- ☐ Worden audittestresultaten vertrouwelijk behandeld en beveiligd opgeslagen?
- ☐ Is er toezicht van de organisatie aanwezig tijdens kritieke audittesten in productie?

Rapportage en opvolging

- ☐ Worden auditbevindingen gerapporteerd aan systeemeigenaar en CISO?
- ☐ Worden kritieke bevindingen direct gecommuniceerd zonder te wachten op het eindrapport?
- ☐ Worden bevindingen aantoonbaar opgevolgd binnen een vastgestelde termijn?



Worden herhaalde bevindingen uit opeenvolgende audits geëscaleerd?

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