Workshop 3 Governance van cybersecurity

1) Analyse Avans IB-beleid: Rollen, taken, verantwoordelijkheden

Rollen & RACI (met Avans governance-context)

Bestuur / College van Bestuur (CvB) – Accountable

- Het CvB is eindverantwoordelijk voor de hogeschoolbrede governance, de naleving van wet- en regelgeving en het beheersen van risico's via een integraal risicomanagementsysteem.
- Het CvB stelt daarnaast een integraal crisisplan vast, inclusief mandaat en taken voor crisisorganen (zoals CMT/LCT).

Raad van Toezicht (RvT) – Oversight / toezicht

- De RvT houdt toezicht op het beleid en de uitvoering door het CvB en ziet toe op naleving van wettelijke verplichtingen.

CISO / Information Security Officer – Responsible (2e lijn)

- De CISO valt binnen de 2e lijn en is verantwoordelijk voor het inhoudelijke kader van informatiebeveiliging: beleid, richtlijnen, monitoring, advies en rapportage richting bestuur.
- De operationele uitvoering van maatregelen ligt primair in de 1e lijn.

Directeuren (organisatieonderdelen/diensteenheden) – Accountable (1e lijn)

- Directeuren zijn verantwoordelijk voor de uitvoering binnen hun organisatieonderdeel en handelen conform Avans beleid en kaders.
- Binnen het Three Lines model ligt bij hen de verantwoordelijkheid om risico's te managen en "in control" te zijn.

(IT-)Operations / Security Operations – Responsible (1e lijn)

- IT-/Security Operations voert de technische controls uit (zoals MFA, logging, patching en monitoring).
- Deze uitvoering valt in de 1e lijn en gebeurt onder verantwoordelijkheid van het lijnmanagement/directie.

BE&C / Concerncontroller – Independent assurance (3e lijn)

- De 3e lijn toetst of beheersmaatregelen/controls daadwerkelijk werken en rapporteert via interne audits en concernanalyses.
- De concerncontroller beoordeelt de opzet en werking van risicobeheersings- en controlesystemen en stuurt BE&C aan.

Functionaris Gegevensbescherming (FG) – Responsible voor AVG-toezicht (onafhankelijk)

- De FG is door het CvB benoemd en houdt onafhankelijk toezicht op naleving van de AVG.
- De FG adviseert het CvB, is contactpersoon voor de Autoriteit Persoonsgegevens en rapporteert periodiek (o.a. halfjaarlijks).

Bestuurssecretaris – Governance & besluitvorming

- De bestuurssecretaris coördineert/monitort het strategisch ambitieplan en voert regie op de overlegstructuur, governance en het besluitvormingsproces van het CvB.
- In besluitvorming bepaalt de bestuurssecretaris of aanvullend advies nodig is (bijv. van BE&C, strategische staf of andere eenheden).

Studenten (incl. studentassessor) – Responsible (veilig gedrag) + input via governance

- Studenten dragen verantwoordelijkheid voor veilig gedrag (o.a. zorgvuldig omgaan met accounts en data, incidenten melden).
- De studentassessor vertegenwoordigt studenten in bestuurlijke/beleidsrijke overleggen en brengt het studentperspectief in.

Leveranciers – Responsible (contractuele security-afspraken)

- Leveranciers zijn verantwoordelijk voor security-afspraken uit contracten/SLA's (zoals beveiligingseisen, incidentmelding en eventueel testen).
- In het bestuursreglement is dit niet gedetailleerd uitgewerkt; dit hoort aanvullend terug te komen in IB-/inkoopbeleid en vormt hier een aandachtspunt ("gap").

Avans beheersmodel: Three Lines (kapstok)

Avans hanteert het **Three Lines model** voor interne beheersing:

- **1e lijn (Doeners):** uitvoering van onderwijs/onderzoek/bedrijfsvoering; directies en teams managen risico's en zijn "in control".
- **2e lijn (Ondersteuners):** beleidsontwikkeling, ondersteuning en monitoring/evaluatie; adviseert 1e lijn en rapporteert instellingsbreed waar nodig.
- **3e lijn (Toetsers):** onafhankelijke toetsing of controls werken; interne audits en concernanalyse via concerncontroller/BE&C.

Mini-checklist “gaten” (aangevuld)

- Eigenaarschap per systeem/proces expliciet? (1e lijn accountable)

- Leveranciers/keten expliciet? *(waarschijnlijk beperkt → noteer als gap)*
- Studenten expliciet genoemd of alleen “gebruikers”? *(koppel aan studentassessor / studentbetrokkenheid)*

- Soft controls zichtbaar (awareness, gedrag, meldcultuur) of vooral techniek?
- Is er een duidelijke route: 1e lijn uitvoeren → 2e lijn monitoren → 3e lijn toetsen?

---

2) OCAI invullen voor Avans (praktische aanpak, zonder extra info nodig)

OCAI meet 4 cultuurtypen:

- **Clan** (mensgericht, betrokkenheid)
- **Adhocratie** (innovatie, experiment)
- **Markt** (resultaat, competitie)
- **Hiërarchie** (regels, structuur, controle)

Hoe vul je het als student “zo eerlijk mogelijk” in?
Gebruik alleen wat je **kunt waarnemen**:

- Communicatie vanuit Avans (mail/portals), toon en prioriteit
- Hoe streng regels zijn (accounts, MFA, toegang, procedures)
- Hoe snel processen werken (support, escalaties)
- Ruimte voor innovatie (projecten, labs, experimenten)

Typische (waarschijnlijke) verdeling voor een hogeschool (startpunt)

- Huidig: **Clan + Hiërarchie** relatief hoog
  (veel samenwerking, maar ook veel regels/beleid)
- Gewenst: iets meer **Adhocratie** (leren/verbeteren) zonder controle kwijt te raken

Tip: Laat elk groepslid OCAI invullen en neem het **gemiddelde**. Dat is meteen “triangulatie”.

---

3) Studentbetrokkenheid bij IB/cyber (soft controls): wat zie je, wat mis je?

Wat je vaak wél ziet (soft controls die "aanwezig" zijn)

- MFA/sterke login → stuurt gedrag afgedwongen (hard control met gedragsimpact)
- Awareness mails / phishing waarschuwingen
- Richtlijnen voor data (bijv. delen van cijfers/gegevens, gebruik van Teams/OneDrive)
- Meldkanalen (servicedesk, security@, incident formulier)

Wat je vaak mist (en dat kun jij als "gap" benoemen)

- Onboarding voor studenten: "veilig werken in 10 minuten" (microlearning)
- Duidelijke "wat te doen bij…?" flows (phishing, verloren laptop, datalek)
- Feedbackloop: studenten melden iets, maar horen nooit de uitkomst → demotiveert melden
- Security-cultuur zichtbaar in onderwijs: concrete voorbeelden per opleiding/project
- "Nudges": reminders op juiste momenten (bij uploaden data, delen links, gastaccounts)

---

4) Posteradvies aan de CISO (soft controls) – kant-en-klare posterinhoud

Je poster kan in 6 blokken (lekker presentabel):

Titel

"Van regels naar gedrag: soft controls die Avans cyberweerbaar maken"

Probleem (1–2 zinnen)

Technische maatregelen zijn sterk, maar incidenten ontstaan vaak door menselijk gedrag (phishing, verkeerd delen, onduidelijk melden).

Observatie als student

- Ik zie: MFA, centrale tooling, waarschuwingen.
- Ik mis: korte onboarding, duidelijke meldpaden, terugkoppeling, "security in de lespraktijk".

Advies (3–5 concrete soft controls)

1. **Student Security Onboarding (10 min)**
   Verplicht bij start studiejaar: phishing, data delen, meldproces, device security.
2. **Meldproces super simpel + zichtbaar**
   1 knop/QR: "Verdacht? Meld het hier." + wat gebeurt er daarna.

3. **Terugkoppeling & beloning van meldgedrag**
   "Je melding hielp ons X te blokkeren" (maandelijks mini-overzicht).
4. **Security nudges in systemen**
   Pop-ups/labels bij delen: "Deel je met externen?" + default veilig.
5. **Docent-toolkit "security by design"**
   1 slide + checklist voor projecten met persoonsgegevens/API's.

Impact (wat levert het op)

- Meer meldingen (vroeger signaleren)
- Minder succes van phishing/social engineering
- Betere naleving AVG en beleid
- Sterkere security-cultuur (veilig gedrag wordt normaal)

KPI's (meetbaar maken)

- % studenten dat onboarding afrondt
- **# phishing meldingen per maand + afhandeltijd**
- Resultaten van phishing simulaties (click-rate omlaag)
- Survey: "Ik weet wat ik moet doen bij incident" ↑