Vragenlijst leveranciersselectie informatiebeveiliging

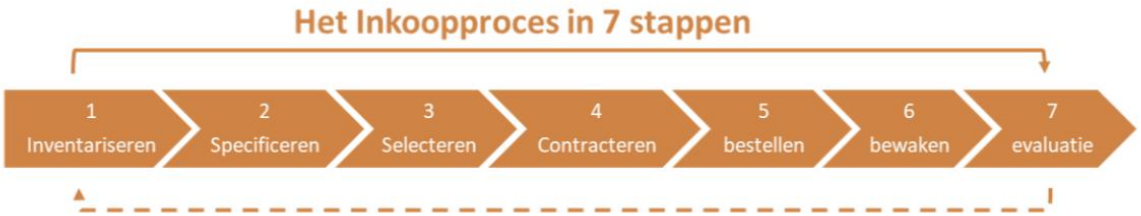
Toelichting

In de precontractuele fase en bij de selectie van een leverancier (dus nog niet de dienst) is het van belang om snel inzicht te krijgen in de volwassenheid van de leverancier op het gebied van informatiebeveiliging. Meer algemene punten zoals *pre-employment screening, verwerkingsovereenkomst,* of *right-to-audit* worden contractueel afgesproken.

Met behulp van de ISO 27002-2022 standaard is een aantal belangrijke informatiebeveiligingseisen geselecteerd. Op basis hiervan zijn vragen geformuleerd die een organisatie kan stellen aan betreffende leveranciers om snel inzicht te krijgen in de security risico's.

Met de verkregen informatie kan worden besloten of de organisatie door wil gaan met de selectie van de dienst (fase 2) en vervolgens contracteren, waarna formele security agreements kunnen worden afgesloten in het contracteringsproces.

In de fasering van Van Weele (zie hieronder), is deze lijst bedoeld voor fase 1.



Voor leveranciers zou het mooi zijn als de onderstaande vragen integraal worden gebruikt door verzekeraars (of financiële instellingen), zodat zij de antwoorden maar één keer hoeven te geven. Verzekeraars hebben dan inzicht in de belangrijkste security vraagstukken en kunnen advies geven aan de contracteigenaren, procurement en/of andere business eigenaren.

Idealiter zit er een iteratie in onderstaande vragenlijst en antwoorden. Door deze bij een aantal verzekeraars te gebruiken samen met leveranciers zal er steeds een verbeterde versie van deze vragenlijst komen.

Security vragen relevant in de precontractuele fase

1. Over welke security certificeringen en assuranceverklaringen beschikt u? *(ISO: 5.19 Information security in supplier relationships)*
2. Beschikt u over een actueel en door het management geaccordeerd informatiebeveiligings- en BCM-beleid? Welke security- en BCM-standaarden zijn hierin opgenomen? Kunt u uw informatiebeveiligings- en BCM-beleid met ons delen? *(ISO: 5.1 Policies for information security)*
3. Hoe ziet uw informatiebeveiligingsorganisatie eruit? Welke functionarissen/afdelingen voor informatiebeveiliging zijn bij u actief (zoals bijv. CISO en een SOC) en wat zijn de rapportagelijnen (bij voorkeur visueel weer te geven)? *(ISO: 5.2 Information security roles and responsibilities)*

4. Heeft u een formeel autorisatiebeleid en -proces ingericht? Kunt u deze met ons delen? *(ISO: 5.3 Segregation of duties)*
5. Heeft u in contracten met leveranciers (en onderaannemers) vastgelegd dat zij aan een vergelijkbaar (met uw eigen instelling/het voor de verleende diensten afgesproken niveau van beveiliging) niveau van informatiebeveiliging moeten voldoen? Is informatie over de data, systemen en diensten beschikbaar in een (of meer) register(s)? *(ISO: 5.9 Inventory of information and other associated assets)*
6. Is uw logische toegangsbeveiliging aantoonbaar ingericht conform het autorisatiebeleid? Waaruit blijkt dit (denk aan een Identity Access Management Systeem)? *(ISO: 5.15 Access control)*
7. Maakt u gebruik van standaard SLA-afspraken en zijn afspraken met betrekking tot informatiebeveiliging en rapportages hierin expliciet inbegrepen (graag een template toevoegen)? *(ISO: 5.19 Information security in supplier relationships)*
8. Beschikt u over een formeel incidentenmanagementproces waarbij klanten onverwijld worden geïnformeerd? *(ISO: 5.26 Response to information security incidents)*
9. Heeft u actuele (IT)-herstelplannen inclusief Business Continuity- en Disaster Recovery Plannen? Zijn deze plannen in de afgelopen 12 maanden getest? Beschikt u over exit-plannen met uw onderaannemers? *(ISO: 5.30 ICT readiness for business continuity)*
10. Beschikt u over een formeel privacy-beleid, is deze beschikbaar en wordt deze aantoonbaar nageleefd? *(ISO: 5.34 Privacy and protection of PII)*
11. Heeft uw organisatie een Secure Development Life Cycle geïmplementeerd en is deze ingericht in lijn met een markt standaard (b.v. Microsoft Security Development Lifecycle (SDL), OpenSAMM, BSIMM, SSE CMM, SafeCode of de NIST SSDF? *(ISO: 8.25 Secure development life cycle)*
    Penetration Testing is onderdeel van deze cyclus. In (assurance, audit) rapporten moet worden aangetoond dat minstens één keer per jaar een pentest is uitgevoerd en dat de bevindingen uit de test zijn opgelost op basis van de ernst van de bevindingen. *(ISO: 8.29 Security testing in development and acceptance)*
12. Beschikt uw organisatie over een security awareness programma en wordt de mate van security awareness van uw medewerkers periodiek gemeten? *(ISO: 6.3 Information security awareness, education and training)*
13. Heeft u een fysiek veiligheidsbeleid en wordt toegang tot kritieke ruimtes (serverruimtes, datacenters, etc.) gemonitord op evt. ongeautoriseerde toegang? *(ISO: 7.4 Physical security monitoring)*
14. Maakt u gebruik van security baselines gebaseerd op marktstandaarden (CIS-benchmarks, NIST, STIG, etc.) of leverancier security-richtlijnen? Zo ja: welke heeft u in gebruik en hoe worden deze gemonitord? *(ISO: 8.9 Configuration management)*
15. Hoe is de (fysieke/virtuele) scheiding (van de verschillende klanten) op netwerkniveau ingericht? *(ISO: 8.22 Segregation of networks)*
16. Voldoen de gebruikte versleuteling technologieën aan de gewenste en gecontracteerde beveiligingsniveaus en is hierbij rekening gehouden met het type, sterkte en kwaliteit van het versleutelingsalgoritme? Welke crypto standaarden heeft u in gebruik? Is hiernaast sleutelbeheer ingericht? *(ISO: 8.24 Use of cryptography)*
17. Maakt u gebruik van gescheiden omgevingen voor ontwikkeling, test, acceptatie en productie. Zijn deze voor iedere klant gescheiden (fysiek of logisch)? *(ISO: 8.31 Separation of development, test and production environments)*
18. Heeft u change management procedures en waarborgen dat alleen geautoriseerd wijzigingen worden geïmplementeerd en hoe zijn security aspecten van deze wijzigingen aangetoond? *(ISO: 8.32 Change management)*