Toelichting team Informatiemanagement en ICT – unit Security

Security maakt momenteel gebruik van Recourse als centrale gouvernance control applicatie voor het ondersteunen van compliance-, audit- en verantwoordingsprocessen voor de Eenduidige Normatiek Single Information Audit (verder: ENSIA) en Wet politiegegevens (verder: WPG). De applicatie wordt ingezet om risico's, maatregelen, controles, bewijslast en bevindingen op een gestructureerde en aantoonbare wijze vast te leggen en te monitoren.

Momenteel wordt Recourse gebruikt voor de uitvoering en verantwoording van onder andere:

- ENSIA (Eenduidige Normatiek Single Information Audit);
- DigiD-steekproeven;
- DigiD-audits;
- Wpg-steekproeven;
- Wpg-audits.

Binnen deze processen worden verschillende normenkaders toegepast. Voor ENSIA betreft dit onder andere de Baseline Informatiebeveiliging Overheid 2 (verder BIO2) en de verantwoordingskaders die onderdeel uitmaken van ENSIA. Voor DigiD worden de actuele DigiD-beveiligingsassessmentnormen toegepast zoals vastgesteld door Logius. Voor de Wpg worden de wettelijke eisen uit de Wpg en de daarbij behorende NOREA audit- en verantwoordingskaders gebruikt. Deze normenkaders vormen de basis voor de inrichting van maatregelen, controles, risico's en auditactiviteiten binnen Recourse.

De applicatie ondersteunt het volledige proces van planning, uitvoering, bewijslastverzameling, monitoring en rapportage. Zowel eerste- als tweedelijnscontroles kunnen worden vastgelegd, waarbij resultaten en bevindingen centraal beschikbaar zijn voor proceseigenaren (beoordelaars), auditors (beoordelaars) en verantwoordelijke en uitvoerende functionarissen (bewijzers).

Onze visie is dat een moderne control-applicatie meer moet bieden dan het registreren van controles. De applicatie dient als integraal platform voor Governance, Risk & Compliance (GRC), waarbij normenkaders, risico's, beheersmaatregelen, controles, audits en verbeteracties door middel van bijv. een mogelijke koppeling met een ticketsysteem met elkaar zijn verbonden. Hierdoor ontstaat een actueel en organisatiebreed inzicht in de mate van compliance en risicobeheersing.

Een belangrijk uitgangspunt is dat wijzigingen die invloed hebben op normenkaders, maatregelen, risico's of controles zo veel mogelijk geautomatiseerd worden verwerkt. Wanneer wet- en regelgeving, normenkaders of auditvereisten wijzigen, verwachten wij dat deze wijzigingen beheerst door de leverancier kunnen worden doorgevoerd binnen de applicatie en direct inzichtelijk zijn voor de betrokken gebruikers. Hiermee wordt de

beheerlast beperkt en blijft de organisatie aantoonbaar werken met de meest actuele eisen, denk bijvoorbeeld aan de cyberbeveiligingswet en de BIO2.

Voor de toekomst zien wij nadrukkelijk mogelijkheden om deze werkwijze verder uit te breiden naar het domein Privacy & Security. Daarbij denken wij aan normenkaders en processen rondom AVG, privacy managementsysteem, privacyrisicoanalyses, DPIA's, informatiebeveiliging, BIO-maatregelen, security-risicomanagement, leveranciersbeoordelingen en periodieke compliance-monitoring. Door deze onderwerpen binnen één geïntegreerde control-applicatie onder te brengen, kan informatie worden hergebruikt, ontstaat een uniforme werkwijze en wordt de aantoonbaarheid van compliance versterkt.

Bij de aanbesteding van een nieuwe GRC-oplossing achten wij het daarom van belang dat de applicatie niet alleen de huidige ENSIA-, DigiD- en Wpg-processen ondersteunt, maar ook voldoende flexibiliteit biedt om gedurende de looptijd van de overeenkomst aanvullende Privacy & Security-functionaliteiten te implementeren. Het doel is te komen tot één centrale omgeving waarin governance, risicomanagement, compliance, privacy en informatiebeveiliging integraal worden ondersteund.

Een belangrijk voordeel van de huidige inrichting is het gebruik van zogenaamde *smart controls*. Hierbij worden beheersmaatregelen en controlevragen gekoppeld aan meerdere normenkaders. Wanneer één controle of bewijslast meerdere normen afdekt, hoeft dezelfde vraag niet afzonderlijk voor ieder normenkader te worden beantwoord. Hierdoor wordt dubbel werk voorkomen, neemt de administratieve belasting af en wordt de kwaliteit en consistentie van de vastgelegde informatie verbeterd. Een controle op bijvoorbeeld toegangsbeheer kan daarmee gelijktijdig bijdragen aan de onderbouwing van eisen uit ENSIA, BIO, DigiD en de Wpg. De applicatie ondersteunt hiermee een geïntegreerde benadering van compliance, waarbij één vastlegging meervoudig kan worden hergebruikt voor verschillende verantwoordings- en auditdoeleinden.