Projectmatig werken heeft de aandacht, niet alleen als het gaat om de toepassing van de methodiek maar ook als het gaan om de ontwikkeling naar een apart projectenbureau binnen de organisatie. Het streven is om van daaruit projecten in de domeinen ruimte, sociaal en bedrijfsvoering te bemensen met projectleiders.

3.4.3 Informatisering en automatisering

Ook in 2025 werken we aan het bij de tijd houden van het gemeentelijke ICT landschap. Een nieuwe financiële applicatie is in gebruik genomen, de gemeentelijke web en telefonievoorzieningen worden vernieuwd, er wordt gekeken naar de realisatie van een E-depot (een voorziening voor het duurzaam bewaren van archiefmateriaal in digitale vorm), et cetera.

Vanzelfsprekend is er daarbij aandacht nodig voor de harde kant van de ICT (applicaties en computerapparatuur). Maar meer en meer verschuift de aandacht naar het document- en gegevenslandschap (samenhang, kwaliteit, vindbaarheid, blijvende beschikbaarheid, de samenhang tussen offline- en online processen en -voorzieningen, samenwerking in ketens met partners en leveranciers, effecten van nieuwe technologie (zoals kunstmatige intelligentie), landelijke ontwikkelingen (zoals Common Ground) en een scala aan wetten (waaronder Woo, Who, AI-act, Eid, Wmebv). We willen daarbij ook meer datagedreven werken, en gegevens ook met onze omgeving delen (denk daarbij aan begrippen zoals ‘smart city’, en ‘open overheid’).

Bij alles wat we doen moeten we scherp sturen op de financiën en op personele capaciteit. In de ICT markt is sprake van forse kostenstijgingen. Technisch en functioneel kan er veel, maar helaas vaak alleen tegen steeds hogere kosten. Ook kan niet alles tegelijk. De personele capaciteit laat dit niet toe. Ook toezien op veiligheid en beveiliging wordt steeds belangrijker en vergt meer tijd.

Leidraad bij afwegingen is dat we moeten voldoen aan wetgeving en dat ontwikkelingen toegevoegde waarde moeten hebben voor de stad en/of de organisatie. Vanzelfsprekend kijken we daar bij ook de aspecten elektronische veiligheid en -robuustheid, IT-control en privacy- en vertrouwelijkheid.

3.4.4 Informatiebeveiliging

Ook in 2025 is de doelstelling om te (blijven) voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Er wordt momenteel gewerkt aan de BIO2.0, welke naar verluidt eind 2024 van kracht zal worden. Een aantal overheidsmaatregelen wordt geactualiseerd in lijn met nieuwe dreigingen (zoals ransomware).

Daarnaast dienen we veranderende wetgeving te volgen. In 2024 vinden veranderingen plaats op het gebied van o.a. de DigiD-audit en het invoeren van een Europese richtlijn om cybersecurity af te dwingen (NIS2).

Omdat het aantal cyberaanvallen (zoals phishing, ransomware en malware) wereldwijd schrikbarend toeneemt, heeft het Europees Parlement ingestemd met het verplichtstellen van NIS2. Met de NIS2 wetgeving wil de Europese Unie een inhaalslag maken met beveiliging tegen cybercriminaliteit. Naar verwachting zal de Cyberbeveiligingswet in 2025 in werking treden, nadat deze door het parlement is behandeld. Organisaties die onder de Cyberbeveiligingswet vallen moeten vanaf dat moment aan de plichten voldoen.

Het voldoen aan bestaande kaders voor informatiebeveiliging bij de overheid, waaronder de BIO, vormt de basis om invulling te geven aan de zorgplicht die uit NIS2 volgt. De wetgeving heeft niet alleen gevolgen voor systemen en toepassingen, maar vooral ook voor werkwijzen, gegevens en documenten.

Jaarlijks onderzoekt een onafhankelijke IT-auditor de verplichte DigiD audit. Vanaf 2024 worden gemeenten naast de bekende 'opzet' en 'bestaan' van beheersingsmaatregelen ook voor drie van de zeven