Toetskader beheer en onderhoud

Adviescollege ICT-toetsing

Toetskader beheer en onderhoud

Inhoudsopgave

Inleiding

Het Adviescollege ICT-toetsing (AcICT) hanteert een toetskader om vast te stellen of het beheer en onderhoud van informatiesystemen doeltreffend en doelmatig is. Het kader is een leidraad bij de onderzoeken die het college uitvoert. De lessen en ervaringen uit onderzoeken van de afgelopen jaren zijn erin verwerkt. Er is een apart toetskader voor ICT-projecten. Beide zijn te vinden op de website van het Adviescollege ICT-toetsing.

De advisering van het Adviescollege ICT-toetsing richt zich onder meer op de doeltreffendheid en doelmatigheid van de beheer- en onderhoudsactiviteiten van een informatiesysteem. Beheer en onderhoud zijn hierbij gedefinieerd als alle activiteiten die worden uitgevoerd voor een informatiesysteem vanaf ingebruikname tot uitfasering.

Het belang van beheer en onderhoud is groot. Het beslaat het grootste deel van de levenscyclus van een informatiesysteem en er zijn de meeste kosten mee gemoeid. Goed uitgevoerd beheer en onderhoud voorkomt verouderde systemen, afnemende flexibiliteit, toenemende kosten en verminderde weerbaarheid. Het uiteindelijke doel is uiteraard om informatiesystemen kwalitatief gezond te houden. Hiermee is beheer en onderhoud de sleutel tot informatiesystemen met een lange levensduur, hoge wendbaarheid en tevreden gebruikers.

Het team van het AcICT gebruikt het Toetskader beheer en onderhoud om de belangrijkste risico's op dit gebied te inventariseren. Het gaat om risico's voor de continuïteit van het informatiesysteem – en daarmee voor de ondersteuning die het systeem biedt. Het toetskader ondersteunt daarnaast CIO-offices binnen het Rijk, eigenaren van informatiesystemen en ICT-afdelingen die operationele informatiesystemen beheren en onderhouden. Met het kader kunnen zij beheer- en onderhoudsrisico's beter beheersen. Aanvullend heeft AcICT voor de belanghebbenden verschillende handreikingen gepubliceerd, bijvoorbeeld over problematische legacy.

Toepassing van het toetskader

Bij een onderzoek naar het beheer en onderhoud stellen we vast in hoeverre een organisatie 'in control' is. Het AcICT toetst aan de hand van twee vragen waarin zeven risicogebieden zijn verwerkt:

1. Ondersteunt het informatiesysteem de doelen van de organisatie en de gebruikers, nu en in de toekomst?
    a. Heeft de organisatie goed zicht op het huidige informatiesysteem en alles wat daarmee samenhangt? (Risicogebied: architectuur)
    b. Zijn de processen voor beheer en onderhoud ingericht? (Risicogebieden: processen, risicobeheersing en leveranciersmanagement)
    c. Is er samenhang met de werkprocessen die worden ondersteund en een heldere visie waar het systeem heen moet de komende jaren? (Risicogebied: samenhang werkprocessen en informatiesysteem)
    d. Zijn verantwoordelijkheden voor beheer en onderhoud belegd? (Risicogebied: eigenaar en ICT-organisatie)
2. Zijn de kosten voor het beheer en onderhoud van het informatiesysteem redelijk? (Risicogebied: financiering)

Ieder risicogebied bevat een aantal toetsaspecten. Ze zijn geformuleerd als principes, niet als specifieke normen, zodat ze toepasbaar zijn op het brede scala van beheer- en onderhoudsvraagstukken. De wijze waarop de toetsaspecten inhoudelijk worden getoetst en gewogen, is afhankelijk van de situatie. Hierbij kan worden gedacht aan het soort informatiesysteem, het maatschappelijk belang voor burgers en bedrijven, de context van de organisatie en het ICT-domein.

Leeswijzer

Dit toetskader bevat zeven hoofdstukken, één per risicogebied. Elk hoofdstuk begint met de relevantie van het risicogebied, gevolgd door een uitwerking van de toetsaspecten.

Waar in dit toetskader 'informatiesysteem' staat, betekent dat één informatiesysteem of een landschap van informatiesystemen met onderlinge koppelingen – en alle techniek die nodig is om dat goed te laten functioneren.

Periodieke aanpassing

Het AcICT herijkt het toetskader periodiek. Daarbij worden nieuwe inzichten, feedback en andere suggesties verwerkt.

1. Architectuur

Actueel inzicht in de architectuur en de gebruikte technologie is voor de ICT-organisatie belangrijk. Dit inzicht is essentieel voor lopend beheer en onderhoud, maar ook voor planning en besluitvorming op de langere termijn.

Toetsaspecten

De aspecten richten zich op drie onderwerpen: actueel inzicht in de architectuur, het beheer van de architectuur zelf en van de technologie.

Actueel inzicht

1. **Er is inzicht in de gebruikte ICT-componenten**
   Er is een actuele registratie die voldoende informatie bevat over alle ICT-componenten (hardware, netwerk, software, AI-modellen, data, koppelvlakken, libraries, frameworks, testscripts, ontwikkeltools) en hun samenhang. Het gaat om informatie die noodzakelijk is voor beheer en onderhoud van het informatiesysteem.

2. **Het is duidelijk in hoeverre het informatiesysteem voldoet aan de gestelde eisen**
   Het is duidelijk aan welke functionele en niet-functionele eisen het informatiesysteem voldoet en hoe en wanneer deze worden getoetst. Hierbij gaat het zowel om specifieke eisen (gerelateerd aan het informatiesysteem) als om algemenere eisen die voortkomen uit wet- en regelgeving (zoals eisen aan informatiebeveiliging en privacy).

3. **De kwaliteit en omvang van het informatiesysteem is bij benadering bekend**
   Er is actueel inzicht in de kwaliteit van het informatiesysteem, waaronder de aanwezige technische schuld en functionele gebreken. De functionele omvang is (bij benadering) bekend en bepaald met behulp van een functiepuntenanalyse of soortgelijke technieken. Deze informatie helpt onder meer bij inschatten van de beheer- en onderhoudslast.

Architectuurbeheer

4. **De architectuur is passend voor het informatiesysteem, ook binnen het bredere ICT-landschap**
   Bij een passende architectuur zijn architectuurkeuzes gemotiveerd en gedocumenteerd vanuit meerdere perspectieven (zoals business, proces, beveiliging, data en infrastructuur). De keuzes komen voort uit de belangrijkste functionele en niet-functionele eisen. De architectuur is duidelijk vastgelegd en traceerbaar naar deze eisen. Er is daarbij rekening gehouden met het bredere ICT-landschap: aanpalende of gekoppelde systemen en ontwikkelingen binnen het landschap en in de betrokken ketens. Bij wijzigingen van eisen wordt vanuit beheer en onderhoud bepaald of deze passen binnen de huidige architectuur of tot architectuurwijzigingen leiden.

5. **Het informatiesysteem is in componenten opgedeeld die apart kunnen worden aangepast en getest**
   Functies zijn optimaal en logisch gegroepeerd over de verschillende componenten, zodat wijzigingen doorgevoerd kunnen worden door slechts één component aan te passen en opnieuw te testen. De componenten zijn op een afgewogen manier ontkoppeld (maximale samenhang, minimale koppeling).

6. **De koppelvlakken worden actief beheerd**
   De specificatie en werking van alle koppelvlakken zijn beschreven en gestandaardiseerd. De gegevensuitwisseling voldoet aan de beveiligingsnormen. Actief beheer zorgt voor monitoring, heldere afspraken voor doorontwikkeling, versiebeheer, modernisering en het bijblijven met actuele standaarden.

Technologie

7. **Het informatiesysteem maakt gebruik van gangbare en volwassen technologie**
   De gebruikte technologie is passend bij het type vraagstuk waarvoor ze ingezet wordt. De technologie wordt nog geruime tijd ondersteund door de leveranciers. Binnen de markt is er voldoende kennis over beschikbaar. Volwassen technologie betekent dat deze al geruime tijd breed en met succes wordt ingezet.

8. **Betrokken partijen hebben voldoende kennis van en ervaring met de technologie**
   De organisatie heeft voldoende kennis van en ervaring met de technologie die wordt gebruikt óf betrekt de

ervaring en kennis van externe partijen. De organisatie heeft expliciet gemaakt welke kennis zij zelf wil bezitten en onderhouden. Bij inhuur van derden beperkt ze de afhankelijkheid.

9. **Er is een planmatige aanpak voor het actueel houden, vervangen en vernieuwen van technische componenten**
   Er is sprake van een planmatige en structurele aanpak van lifecyclemanagement voor alle componenten relevant voor het informatiesysteem. Dit omvat in ieder geval data, gebruikte AI-modellen, software (inclusief libraries en ontwikkelplatformen), hardware, netwerkcomponenten en koppelvlakken.

Internationale standaarden

Zie Toetskader projecten, https://www.adviescollegeicttoetsing.nl/onze-werkwijze/toetskader/toetskader1

Rijksstandaarden en methodieken

- Forum Standaardisatie: Verplichte en aanbevolen standaarden t.a.v. koppelvlakken en technologie, https://forumstandaardisatie.nl/
- Nederlandse Overheid Referentie Architectuur (NORA), https://www.noraonline.nl/wiki/NORA_online
- Kenniscentrum voor beleid en regelgeving: DPIA, https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/beleidskompas/verplichte-kwaliteitseisen/data-protection-impact-assessment

Interessante publicaties en artikelen

- Steve McConnel, Software Estimation: Demystifying the Black Art
- Wat is een “Software Bill of Materials”?, https://www.digitaltrustcenter.nl/wat-is-een-sbom
- ‘Goede voorbeelden op het gebied van softwareontwikkeling’; (2020) CIO-Rijk, https://www.tweedekamer.nl/downloads/document?id=2020D52487
- Architecture Improvement Method – AIM42, https://aim42.github.io/
- Migrating Legacy Systems: Gateways, Interfaces and the Incremental Approach, Brodie/Stonebraker, 1995
- Working effectively with legacy code, Michael Feathers, 2006
- B. Beyer, C. Jones, J. Petoff, andN. R. Murphy, Site reliability engineering: How Google runs production systems. O’Reilly Media, Inc., 2016.

2. Processen

Beheer-, onderhoud- en voortbrengingsprocessen zijn belangrijk om de stabiliteit, betrouwbaarheid en veiligheid van informatiesystemen te waarborgen. Een goede inrichting van deze processen zorgt voor een gestructureerde aanpak van de kwaliteits- en risicobeheersing.

Toetsaspecten

Er zijn ingerichte en werkende processen voor beheer en onderhoud op strategisch, tactisch en operationeel niveau. Voor wijzigingen zijn er werkende 'voortbrengingsprocessen'.

1. **Op strategisch niveau**
   Op strategisch niveau heeft de organisatie processen gedefinieerd die het systeem op de langere termijn gezond houden. Eisen die voortkomen uit werkprocessen en wet- en regelgeving zijn daarbij leidend. De processen op strategisch niveau bevatten in elk geval de volgende activiteiten/onderdelen:

   - **Er is een meerjarige ICT-visie en -strategie**
     Deze omvat in ieder geval strategische doelstellingen, principes en uitgangspunten die leidend zijn voor beheer en onderhoud.

   - **Er is een roadmap gericht op het bereiken van strategische doelstellingen**
     De roadmap wordt periodiek bijgesteld zodat de activiteiten en het gebruik van de (schaarse) middelen in balans zijn en blijven. Dit proces bestaat uit inventarisatie, registratie en actualisatie van wijzigingen in informatiesystemen. Ook vastlegging van de ontwikkeling van de onderdelen hoort daarbij.

   - **Informatiesystemen worden tijdig geactualiseerd, vernieuwd of vervangen**
     Dit blijkt uit de langetermijnplanning en zorgt ervoor dat systemen veilig, efficiënt en up-to-date blijven gedurende hun hele levensduur.

   - **Er is een duidelijke strategie die bepaalt wie werkzaamheden uitvoert en waar**
     Deze strategie zorgt voor een bewuste keuze – gebaseerd op kosten, kennis en risico's – voor zelf werkzaamheden uitvoeren, in samenwerking met anderen, óf uitbesteding ervan aan een overheidsorganisatie of marktpartij.

2. **Op tactisch niveau**
   Op tactisch niveau worden de uitkomsten van de strategische processen vertaald naar meer concrete werkprocessen, services en middelen. Het gaat hierbij bijvoorbeeld om processen voor kwaliteitsbeheer van de ICT-dienstverlening, voor het managen van risico's, voor het plannen van capaciteit, voor het garanderen van de performance en voor de informatiebeveiliging en de continuïteitsborging.

   De processen op tactisch niveau bevatten in elk geval de volgende onderdelen:

   - **Er zijn plannen voor uitval en uitwijk**
     Er is een proces dat ervoor zorgt dat een informatiesysteem kan blijven functioneren na een verstoring of uitval. Het plan bevat de identificatie van potentiële risico's voor de continuïteit, strategieën om die risico's te mitigeren en geteste plannen voor uitval en uitwijk.

   - **Informatiebeveiliging krijgt structureel aandacht**
     Hierbij gaat het om het proces van het beschermen van informatie, systemen en netwerken tegen bedreigingen van de vertrouwelijkheid, integriteit en beschikbaarheid ervan. Het proces omvat het proactief en reactief ontwikkelen en implementeren van beleid, procedures en technische maatregelen.

   - **Capaciteit en performance worden beheerst**
     Er is een planning van en aandacht voor de optimalisatie van de benodigde capaciteit en performance van IT-middelen ten behoeve van rekenkracht, opslag en bandbreedte.

- **Kwaliteit van dienstverlening wordt bewaakt**
  De kwaliteit van dienstverlening aan interne en externe afnemers is gedefinieerd en wordt gemeten, beheerst en bewaakt.
- **Er is een planning (en regelmatige actualisering) van de activiteiten voor beheer en onderhoud**
  De planning en voortgang van activiteiten is inzichtelijk en actueel. Waar nodig wordt afgestemd met betrokken partijen. De planning is gebaseerd op ervaring en/of beschikbare kengetallen en houdt rekening met tegenvallers.

3. **Op operationeel niveau**
   Op het operationele niveau gaat het om de dagelijkse uitvoering van IT-werkzaamheden: het laten functioneren en ondersteunen van systemen, oplossen van verstoringen, doorvoeren van wijzigingen en leveren van IT-diensten aan eindgebruikers. Hier worden de plannen en processen van het tactische niveau in de praktijk gebracht.

   De processen op operationeel niveau zorgen in ieder geval voor:

   - **Monitoring van applicatie en infrastructuur**
     Applicatie en infrastructuur worden gemonitord op capaciteit- en middelenbeslag en op beveiliging. Dit voorkomt knelpunten en signaleert incidenten vroegtijdig.

   - **Gestructureerde aanpak van incidenten en problemen**
     Incidenten worden geregistreerd, opgelost en gemonitord. Terugkerende incidenten worden verder geanalyseerd om de achterliggende oorzaken aan te pakken.

   - **Gecontroleerde doorvoering van wijzigingen**
     Er is een proces dat wijzigingen beoordeelt op risico's, de wijzigingen autoriseert, inplant, (geautomatiseerd) test en implementeert. Hierdoor kunnen verstoringen, incidenten en herstelwerkzaamheden tot een minimum beperkt blijven.

4. **Voortbrengingsprocessen**

   Bij wijzigingen zijn er ingerichte en werkende voortbrengingsprocessen waarbij in ieder geval de volgende principes leidend zijn:

   - **De ontwerp-bouw-test-implementatie-cyclus is zo kort mogelijk**
     Het voortbrengingsproces faciliteert kortcyclische oplevering en ingebruikname van bruikbare (deel)producten die voldoen aan de gestelde eisen.

   - **De ontwikkelwerkwijze faciliteert tijdige betrokkenheid van gebruikers om functionaliteit te toetsen**
     De ontwikkelwerkwijze omvat alle activiteiten voor specificeren, ontwerpen, ontwikkelen, testen en uitrollen om tot een werkende oplossing te komen. Zowel interne gebruikers (binnen de organisatie) als externe (burgers als dat van toepassing is) worden tijdig betrokken om vast te stellen of de te ontwikkelen of aangepaste functionaliteiten voor hen bruikbaar zijn en passen bij wat zij nodig hebben.

   - **De ontwikkelwerkwijze is passend**
     De ontwikkelwerkwijze is duidelijk voor de belanghebbenden binnen en buiten de ICT-organisatie en past bij de aard van de opgave, het type informatiesysteem en de context. Daarbij hebben betrokken mensen voldoende ervaring met de werkwijze en met de juiste toepassing. De ontwikkeling wordt ondersteund door geautomatiseerde processen voor bijvoorbeeld testen en installeren.

   - **Omvangrijke wijzigingen worden projectmatig opgepakt**
     Wijzigingen die zo omvangrijk zijn dat ze grote impact hebben op het informatiesysteem, de begroting en/of de organisatie worden projectmatig opgepakt. Daarbij wordt de beheerorganisatie betrokken en de aanwezige expertise benut. Zie hiervoor het toetskader voor projecten.

Internationale standaarden

- Software engineering process, models, methods, quality: Software Engineering Body of Knowledge (SWEBOK) https://www.computer.org/education/bodies-of-knowledge/software-engineering
- Cost Estimating Body of Knowledge - Software (CEBoK-S), https://www.iceaaonline.com/cebok-s/
- Testmethodieken: Test Management Approach (TMap), https://www.testlearning.net/en/tmap
- Planningsmethodieken: Reference Class Forecasting, https://en.wikipedia.org/wiki/Reference_class_forecasting
- BiSL (Business Information Services Library), https://bislfoundation.nl/het-model/
- ITIL, ITIL® Foundation: ITIL 4 edition, Axelos, 2019
- Information technology — Service management, ISO/IEC 20000-1:2018
- Software engineering — Software life cycle processes — Maintenance, ISO/IEC/IEEE 14764:2022
- DORA-metrics, https://dora.dev/guides/

Rijksstandaarden en methodieken

- Beoordelingskader IT lifecyclemanagement, Algemene Rekenkamer, https://www.rekenkamer.nl/onderwerpen/verantwoordingsonderzoek/over-dit-onderzoek/beoordelingskaders/beoordelingskader-it-lifecyclemanagement

Interessante publicaties en artikelen

- Handreiking over legacy, Adviescollege ICT-toetsing, 2025, https://www.adviescollegeicttoetsing.nl/documenten/2025/03/19/handreiking-legacy
- De Scrum Gids; Schwaber, K. en Sutherland, J. (2020) https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-Dutch.pdf
- The Economics of Software Quality; Jones, C. en Bonsignour, O. (2012), Addison-Wesley.
- Software Economics and Function Point Metrics: Thirty years of IFPUG Progress, Version 10.0; Jones, C. (April 14, 2017), https://www.ifpug.org/wp-content/uploads/2017/04/IYSM.-Thirty-years-of-IFPUG.-Software-Economics-and-Function-Point-Metrics-Capers-Jones.pdf
- Accelerate: The Science of Lean Software and DevOps, Nicole Forsgren, Jez Humble, Gene Kim, 2018.

3. Risicobeheersing

Het beheer en onderhoud van informatiesystemen kent diverse risico's. Het is belangrijk om inzicht te hebben in de relevante risico's en om ze te beheersen.

Toetsaspecten

1. **Risicobeheersing is structureel verankerd**
   De eigenaar van het informatiesysteem en het management van de beheersorganisatie hebben structureel oog voor risico's op het gebied van beheer en onderhoud. Het gaat om risico's enerzijds op politiek, bestuurlijk, juridisch en organisatorisch niveau, anderzijds op operationeel en technisch niveau. Op basis van periodieke risicoanalyses worden de risico's in beeld gebracht en worden mitigerende maatregelen met de juiste urgentie opgepakt. Dit is een continu proces.

2. **De organisatie bewaakt de effectiviteit van de getroffen maatregelen**
   Omdat de omgeving en de organisatie gedurende de tijd kunnen veranderen, wordt de effectiviteit van maatregelen die risico's inperken, structureel gemonitord. De beheersorganisatie stelt ze zo nodig bij.

3. **Er is openheid en transparantie over risico's**
   Als medewerkers van de organisatie risico's delen, geeft dit kansen om ze effectief te identificeren, toe te wijzen en er maatregelen tegen te nemen.

4. **Er is voldoende aandacht voor risico's voor informatiebeveiliging en strategische digitale veiligheid**
   In de risicobeheersing rond het informatiesysteem krijgt informatiebeveiliging voldoende aandacht. Bij het uitvoeren van risicoanalyses wordt ook bepaald wat de kans is op inbreuk en (gegevens)diefstal door statelijke actoren, georganiseerde misdaad en eventueel hacktivisten of extremistische groepen.

5. **Risico's door afhankelijkheden van ketenpartners worden beheerst**
   De organisatie heeft inzicht in afhankelijkheden van bijvoorbeeld projecten, ketenafspraken, releases van andere informatiesystemen, relaties met wet- en regelgeving, en diensten van en koppelvlakken met derden.

6. **Continuïteits- en concentratierisico's krijgen voldoende aandacht**
   Continuïteits- en concentratierisico's met betrekking tot leveranciers waarvan het informatiesysteem afhankelijk is, worden geadresseerd in het risicomanagement.

Internationale standaarden

- Informatiebeveiliging, ISO/IEC 27001 & 27002
- Risico Management, ISO 31000:2018
- Enterprise Risk Management — Integrated Framework, COSO 2017 https://www.coso.org/
- COBIT, COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2019
- NIS2, https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/

Rijksstandaarden en methodieken

- Routekaart Risicomanagement Nationaal Cyber Security Centrum, https://www.digitaleoverheid.nl/nieuws/routekaart-risicomanagement/
- Baseline Informatiebeveiliging Overheid (BIO2) , https://www.bio-overheid.nl/

Interessante publicaties en artikelen

- Toetsingskader Algoritmes, Algemene Rekenkamer, https://www.rekenkamer.nl/onderwerpen/algoritmes/toetsingskader
- DORA , https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
- Handreiking Cybersecurity voor Bestuurders en Bedrijfseigenaren, Cyber Security Raad , https://www.cybersecurityraad.nl/documenten/2025/06/04/handreiking-cybersecurity-voor-bestuurders-en-bedrijfseigenaren

4. Leveranciersmanagement

Bij inkoop en aanbesteding worden keuzes en (financiële) afspraken met marktpartij(en) gemaakt die impact hebben op beheer en onderhoud. Het is dan ook belangrijk om heldere contractafspraken te maken en passende stuurmiddelen in te richten.

Toetsaspecten

1. **Contracten en afspraken zijn inzichtelijk en worden onderhouden**
   Afspraken met leveranciers zijn beschreven in contracten en dienstverleningsovereenkomsten. Hierin staan concreet en meetbaar de afspraken en wederzijdse verplichtingen, waaronder het recht op controle en audit. Er is een actueel inzicht in alle lopende contracten inclusief de daarbij betrokken onderleveranciers. De samenwerking tussen opdrachtgever en leverancier wordt periodiek geëvalueerd en de uitkomsten komen in een contractdossier. De doelmatigheid van contracten wordt periodiek geëvalueerd.

2. **De beheerorganisatie kan sturen op gemaakte afspraken**
   De kwaliteit van dienstverlening is gedefinieerd en wordt gemeten, beheerst en bewaakt. De beheerorganisatie ziet erop toe dat leveranciers hun afspraken nakomen. Doet een leverancier dit niet, dan moet duidelijk zijn voor betrokken partijen wat de oorzaak is en wat de consequenties zijn, zowel financieel als voor de ondersteuning van het informatiesysteem. Binnen de organisatie is voldoende kennis aanwezig om een gelijkwaardig gesprek te voeren met leveranciers.

3. **Er is een exit-strategie**
   Er moet een vooraf opgestelde exit-strategie zijn voor de afgesloten contracten. In die strategie staat minimaal wat de alternatieve leveranciers of producten zijn en hoe de migratie van informatiesystemen en data er op hoofdlijnen uitziet. De afspraken hierover zijn ook in de daarvoor relevante contracten opgenomen.

4. **Afspraken voorzien in overdracht naar een andere leverancier**
   Alles wat nodig is om het informatiesysteem te kunnen beheren, onderhouden en exploiteren, moet kunnen worden overgedragen naar een andere leverancier. Het gaat hierbij in ieder geval om de software, de data, documentatie, testsets, benodigde infrastructuur en de gereedschappen. De overdracht is mogelijk zonder licentiebeperkingen op software, beperkingen op het vlak van intellectueel eigendom of een dermate hoge kennisdrempel dat effectief onderhoud door een andere leverancier niet mogelijk is. Ook zijn de beperkingen voor overdraagbaarheid op infrastructuurniveau geminimaliseerd en is er rekening gehouden met de mogelijke overdracht naar een andere leverancier.

5. **Hercontractering wordt tijdig voorbereid en gestart**
   Bij contactverlenging of -vernieuwing wordt rekening gehouden met de richtlijnen voor aanbestedingen. Om de continuïteit van de ICT-dienstverlening te garanderen, start de organisatie tijdig met de voorbereiding voor een aanbesteding.

Internationale standaarden

- Overdragen van software, NPR 5325:2017
- Cybersecurity, Supplier relationships, Part 3: Guidelines for hardware, software, and services supply chain security, ISO/IEC 27036-3:2023
- Relevante onderdelen binnen ITIL4 (Supplier Management) en COBIT (COBIT APO10.03 - Manage Vendor Relationships And Contracts)
- Guidance on outsourcing, ISO 37500:2014

Rijksstandaarden en methodieken

- Afwegingskader ICT-opdrachten, CIO-Rijk (2020)
  https://www.tweedekamer.nl/downloads/document?id=2020D52489
- Strategisch Leveranciersmanagement voor de Rijksoverheid , https://slmmicrosoftrijk.nl/
- Handleiding Publieke Sector Comparator van het ministerie van Financiën
  https://open.overheid.nl/documenten/ronl-archief-c63c6292-496d-4cde-b52d-d3911a2c49ef/pdf

Interessante publicaties en artikelen

- Handreiking leveranciersmanagement Adviescollege ICT-toetsing, https://www.adviescollegeicttoetsing.nl/documenten/2021/12/14/handreiking-leveranciersmanagement
- Vaststellen betrouwbaarheid van clouddiensten: Online Trust Coalition https://ecp.nl/project/online-trust-coalitie/

5. Samenhang werkprocessen en informatiesysteem

Het informatiesysteem moet uiteraard passen bij de te ondersteunen werkprocessen. In de beheer- en onderhoudsaanpak is expliciet aandacht voor de blijvende aansluiting tussen deze twee. Bij gebruikers kan het ook gaan om burgers die gebruik maken van dienstverlening die met het informatiesysteem wordt geleverd.

Toetsaspecten

1. **De werkprocessen en het informatiesysteem worden in samenhang doorontwikkeld**
   Verbetering en optimalisering van de werkprocessen en het informatiesysteem gebeuren in samenhang. Er wordt tijdig geanticipeerd op veranderingen in werkprocessen en op veranderingen in de technologie.

2. **Doorontwikkeling gebeurt samen met de gebruikers**
   Een vertegenwoordiging van de gebruikers is actief betrokken bij de doorontwikkeling van (nieuwe) werkprocessen en bijbehorende aanpassingen aan het informatiesysteem. Als het informatiesysteem een belemmerende factor is voor de gewenste aanpassing van de werkprocessen, zoeken de ontwikkelaars in afstemming met de gebruikersorganisatie naar alternatieven. Anderzijds, als complexiteit en kosten van de informatiesystemen significant verlaagd kunnen worden door redelijke wijzigingen in werkprocessen, dan wordt de gebruiksorganisatie gevraagd dit te overwegen.

3. **Bij wijzigingen is er aandacht voor implementatie in de gebruikersorganisatie**
   Bij grotere wijzigingen is er aandacht voor de implementatie in de gebruikersorganisatie. Instructies en opleidingen ondersteunen de gebruikers bij de ingebruikname. Hun feedback wordt geregistreerd en verwerkt.

Internationale standaarden

- Business Process Model and Notation, BPMN 2.0, https://www.bpmn.org/

Rijksstandaarden en methodieken

- Beleidskompas, https://www.kcbr.nl/beleid-en-regelgeving-ontwikkelen/beleidskompas
- Digitale Toets Tweede Kamer, bijlage bij brief commissie; Openbaarmaking van het verslag van de rapporteurs over Digitale rechtsstaat, 26.643, TK, 1361, 2 juli 2025
- Digitale Toets Raad van State, https://www.raadvanstate.nl/overrvs/advisering/beoordelingskader/uitgebreide-toelichting-van-de-toets-van/

Interessante publicaties en artikelen

- Community Gebruiker Centraal , https://www.gebruikercentraal.nl/

6. Eigenaar en ICT-organisatie

Voor de continuïteit van een informatiesysteem – en daarmee voor het beheer en onderhoud – is de invulling van het eigenaarschap ervan belangrijk. Bovendien vraagt beheer en onderhoud om een beheersorganisatie: een organisatieonderdeel dat de activiteiten uitvoert en de eigenaar van het informatiesysteem ondersteunt.

Toetsaspecten

De aspecten richten zich op het eigenaarschap en op de beheersorganisatie.

Eigenaarschap

1. **De eigenaar is verantwoordelijk voor de continuïteit en het beheer van het informatiesysteem**
   De eigenaar is verantwoordelijk en neemt deze verantwoordelijkheid ook. De eigenaar formuleert de eisen waar het informatiesysteem aan moet voldoen, stelt het gewenste dienstverleningsniveau vast, laat zich voldoende informeren door de ICT-organisatie en richt de benodigde sturing in.

2. **De eigenaar stelt de langetermijnvisie vast**
   De eigenaar is inhoudelijk betrokken bij de langetermijnvisie op beheer en onderhoud van het informatiesysteem, en stelt deze ook vast.

3. **De eigenaar is inhoudelijk op de hoogte**
   De eigenaar heeft voldoende inhoudelijke kennis van zowel de te ondersteunen werkprocessen als het informatiesysteem. De eigenaar is ook voldoende inhoudelijk op de hoogte van de risico's en de kwaliteit van het systeem.

Organisatie

4. **De rollen, taken, verantwoordelijkheden en bevoegdheden in de organisatie zijn duidelijk**
   Voor betrokkenen bij het beheer en onderhoud is duidelijk wat van hen verwacht wordt en wat hun mandaat is. Dat geldt ook voor activiteiten die zijn uitbesteed aan derden.

5. **De organisatie bestaat uit mensen met voldoende kennis en ervaring**
   Er is voldoende kennis en ervaring in de organisatie aanwezig of beschikbaar van derden om de taken op het gebied van beheer en onderhoud (blijvend) te kunnen uitvoeren. Denk hierbij aan domeinkennis, functionele kennis en ervaring met beheersprocessen.

6. **De organisatie bevordert open communicatie en samenwerking**
   De communicatie is open en de samenwerking binnen de organisatie en met belanghebbenden is effectief. Zo is tijdige bijsturing mogelijk.

7. **Er is aantoonbaar en structureel ruimte voor 'tegendenken' en een kritische blik**
   Er is in de organisatie voldoende ruimte voor discussie en tegenspraak. Ook is er voldoende inbreng van buitenstaanders op de manier van werken en op het bepalen van de kwaliteit van het informatiesysteem.

Internationale standaarden

Zie verwijzing bij onderdeel processen.

Rijksstandaarden en methodieken

- Handboek Portfoliomanagement Rijk, CIO-Rijk

Interessante publicaties en artikelen

Zie verwijzing bij onderdeel processen.

7. Financiering

Voor goed beheer en onderhoud van een informatiesysteem gedurende de hele levenscyclus is passende dekking van de kosten nodig. De financiering wordt op regelmatige basis geëvalueerd en zo nodig bijgesteld. De organisatie zorgt voor een efficiënte besteding van de beschikbare middelen.

Toetsaspecten

1. **Er is een vastgestelde meerjarenbegroting**
   De begroting voor beheer en onderhoud is vastgesteld en is toereikend voor alle beheer- en onderhoudsactiviteiten. De begroting bevat alle kostensoorten van het informatiesysteem, inclusief de onderliggende infrastructuur, de benodigde licenties en de kosten van het te verwachten gebruik. Daarbij wordt rekening gehouden met verwachte aanpassingen, doorontwikkeling, innovatie en de afschrijving van componenten op de korte en lange termijn. Ook een eventuele uitfasering en het reserveren van middelen voor vervanging horen erbij.

2. **De begroting wordt periodiek herijkt**
   De organisatie analyseert en verklaart afwijkingen van de feitelijke uitgaven ten opzichte van het budget. Ze evalueert regelmatig gebruikte normbedragen en past die waar nodig aan. Beide vormen input voor de herijking van de begroting.

3. **De verantwoordelijken hebben mogelijkheden om te sturen op de besteding van het budget**
   Het is duidelijk welke activiteiten tot welke kosten leiden en wie daarover kan en mag beslissen. Het inzicht is op voldoende detailniveau om daarop te kunnen sturen. Bij grootschalig onderhoud worden alternatieve oplossingen aangeboden ter besluitvorming, inclusief een kosten-batenraming.

4. **Het beheer en onderhoud is kostenefficiënt**
   Het beheer en onderhoud presteert volgens afgesproken doelstellingen en prestatiecriteria tegen zo laag mogelijke kosten.

Internationale standaarden
Zie toetskader projecten.

Rijksstandaarden en methodieken
- Rijks ICT-dashboard https://www.rijksictdashboard.nl/

Interessante publicaties en artikelen
- Handreiking baten management, Adviescollege ICT-toetsing, https://www.adviescollegeicttoetsing.nl/documenten/2024/10/30/handreiking-batenmanagement
- Applied Software Measurement, Global Analysis of Productivity and Quality, Caper Jones, 2008
- Software Estimation: Demystifying the Black Art, Steve Mconnell, 2006
- ISO/IEC/IEEE 14764:2022 - Software life cycle processes Maintenance

Deze publicatie is een uitgave van:

Adviescollege ICT-toetsing
info@adviescollegeicttoetsing.nl
www.adviescollegeicttoetsing.nl
Postbus 16292 | 2500 BG Den Haag

29 september 2025

Adviescollege
ICT-toetsing