# ACBIT Risicoanalyse

**Onderdeel van de ACBIT, Algemene Corporatie Inkoopvoorwaarden bij IT**

*December 2021*

# Colofon



**Redactie en vormgeving:**
Aedes vereniging van woningcorporaties

**Contact en meer informatie:**
Gaby van der Peijl, adviseur opdrachtgeverschap & inkoop, g.vanderpeijl@aedes.nl, 06 351 124 59

**Disclaimer**

De ACBIT risicoanalyse is onderdeel van de algemene corporatievoorwaarden bij IT. De ACBIT-toolbox bestaat uit onder andere: de ACBIT 2021 Inkoopvoorwaarden, een toelichting op de voorwaarden en een overeenkomstengenerator. De toolbox is met zorg en aandacht opgesteld. Er is geen garantie dat de informatie juist is op het moment waarop zij wordt ontvangen, of dat de informatie na verloop van tijd nog steeds juist is. De gebruikers van de toolbox zijn zelf verantwoordelijk voor de juiste toepassing en kunnen er geen rechten ontlenen aan de toolbox. Er wordt geen aansprakelijkheid aanvaard voor schade als gevolg van onjuistheden en/of gedateerde informatie.

# INHOUD

# INLEIDING

De ACBIT is een set uniforme en gestandaardiseerde inkoopvoorwaarden die woningcorporaties en samenwerkingsverbanden kunnen gebruiken bij de inkoop van ICT-producten of -diensten. Een nadere specificatie van het toepassingsgebied van de ACBIT is beschreven in de toelichting bij de voorwaarden. In de inleiding leggen we de link tussen de ACBIT en de risicoanalyse.

## 1.1. ACBIT en de risicoanalyse

Voor Opdrachtgevers is het van belang dat een in te kopen ICT-product of -dienst aansluit bij het gebruikte Applicatielandschap. In artikel 3 van de ACBIT komt de precontractuele zorgplicht van de Leverancier duidelijk naar voren. De ACBIT vult de zorgplicht voor wat betreft de voorfase van contracteren nader in. Leverancier moet zich namelijk niet alleen goed op de hoogte stellen van relevante informatie over Opdrachtgever en het voorgenomen project (artikel 3.2/3.3), maar daar vervolgens ook wat mee doen door deze informatie te vertalen in het aanbod en de risicoanalyse (artikel 3.4/3.5). Van Leverancier wordt in feite verwacht dat hij voldoet aan het 'ken uw klant' en 'ken uw product' principe. Doordat Leverancier de Opdrachtgever moet waarschuwen voor eventueel gesignaleerde risico's, wordt bovendien bewerkstelligd dat Opdrachtgever vooraf weet met welke risico's rekening gehouden moet worden.

De gedachte is dat de inventarisatie van risico's zo meer naar voren wordt gehaald en beide partijen beter weten waar ze aan beginnen en vroegtijdig mitigerende maatregelen kunnen treffen. De aard en omvang van de risicoanalyse zal per opdracht verschillen. Bij kleine opdrachten of projecten is denkbaar dat de inventarisatie nauwelijks iets om het lijf heeft en bij wijze van spreken beperkt blijft tot het uitdrukkelijk wijzen op de systeemeisen en navraag doen naar gebruik van bij Leverancier bekende incompatibele combinaties van hard- en software. Bij grote opdrachten en projecten zal hier meer van beide partijen gevergd worden. Nuance en maatwerk blijven terugkerende thema's, ook hier. Het gaat inderdaad niet alleen om de grootte van de opdracht, maar ook de voorzienbaarheid en bekendheid van risico's. Kleine opdrachten, waarvan bekend is dat zij veel risico in zich dragen, leidt ook tot een zwaardere plicht dit vooraf te melden.

## 1.2. Opdrachtgeverschap en inkoop

Aedes benadrukt dat als je de ACBIT gebruikt, je deze niet 1 op 1 kunt overnemen. Het is noodzakelijk om continu te bedenken: wat heeft de corporatie nodig en hoe willen wij dat organiseren. Vragen die je je bij het gebruik van de risicoanalyse kunt stellen zijn:

- Wat zijn mijn organisatiedoelstellingen.
- Welke ICT Prestatie wil ik graag verbeteren.
- Is de ICT Prestatie betrouwbaar, of varieert het kwaliteitsniveau.
- Wat is de oorzaak van mogelijke ICT kwaliteitsproblemen.
- Welke gegevensstandaarden kan ik gebruiken.
- Hoe zorg ik dat de ICT kwaliteitsproblemen niet terugkomen.
- Past de ICT Prestatie voldoende bij de corporatietaken.
- Met welke andere interne en externe (toekomstige) systemen komt de ICT Prestatie in verbinding te staan.
- Zijn er vanuit de huidige systemen afhankelijkheden om rekening mee te houden. Denk bijvoorbeeld aan reeds ingeregelde processen of data.

- Op welke wijze dient de ICT-oplossing data te ontvangen, te genereren en op te slaan. En wat wil de corporatie met deze data doen.
- Wat zijn mogelijke toekomstige ontwikkelingen, bijvoorbeeld ten aanzien van de wensen van gebruikers, technologische ontwikkelingen en wanneer gewisseld wordt van leverancier.

Dit zijn ook vragen die bij het inrichten van het inkoopproces en contractmanagement aan de orde komen. Voor professioneel opdrachtgeverschap en inkoop heeft Aedes verschillende leidraden, handleidingen en standaarddocumenten beschikbaar. In 2022 komt er een uitbreiding op de ACBIT. Dit gaat onder andere om een strategiedocument en vraagspecificatie.

## 1.3. Opdrachtgeverschap en risicoanalyse

Bij zeer risicovolle en complexe projecten ligt het voor de hand separaat advies in te winnen over de risico's. Hetzij bij Leverancier zelf als afzonderlijke (deel)opdracht, hetzij bij een derde partij. In dit soort gevallen is er echter geen sprake meer van een precontractuele verplichting. Het is nu een opdracht geworden waar een factuur tegenover staat. Dit kan zeker voor risicovolle en complexe projecten wenselijk zijn.

Steeds moet worden bedacht dat de risicoanalyse een invulling is van de precontractuele zorgplicht. Deze analyse gaat dus ook niet verder dan wat er redelijkerwijs precontractueel van een leverancier mag worden verwacht. Juist een Leverancier die zijn eigen product kent, kan in voorkomend geval er tijdig voor waarschuwen (en ook goed uitleggen) dat een goede risicoanalyse dusdanig veel tijd en moeite kost dat het in dat specifieke geval niet redelijk is dit te beschouwen als onderdeel van de offertefase. In de meeste gevallen zal deze precontractuele verplichting vallen binnen wat er redelijkerwijs van een Leverancier mag worden verwacht.

Hierbij moet ook benadrukt worden dat Opdrachtgever medewerking moet verlenen aan de risicoanalyse, door de redelijkerwijs gevraagde informatie aan te leveren (artikel 3.3). Bij een gebrek aan medewerking door Opdrachtgever kan van Leverancier niet meer worden verwacht dan dat deze zijn aanbod doet op basis van de wel beschikbare informatie. Leveranciers doen er zodoende goed aan te documenteren, en liefst te expliciteren, op basis van welke informatie zij hun aanbod doen. Dit maakt voor beide partijen duidelijk wat de basis voor de samenwerking vormt.

Afhankelijk van de waarde van de opdracht en/of het eigen inkoopbeleid van woningcorporaties zal een opdracht aanbesteed moeten worden De aanbestedingswetgeving beperkt de ruimte voor leveranciers om zelf bij opdrachtgevers tijdens het aanbestedingsproces navraag te doen. Dit wordt erkend in artikel 3.5 van de ACBIT. In dit geval dient alle relevante informatie die nodig is voor de Leverancier in de aanbestedingsstukken te zijn opgenomen.

Uiteraard moet de Leverancier in de nota van inlichtingen om aanvullende informatie vragen wanneer de aanbestedingstukken niet duidelijk genoeg antwoord geven op bepaalde vragen.

## 1.4. Leeswijzer

Dit document beschrijft allereerst hoe de risicoanalyse is opgebouwd. Vervolgens volgen voorbeelden van risico's. Moet je alle risico's beheersen? Nee, we raden aan om hier zorgvuldige keuzes in te maken. De bedreigingen (risico's) beschrijf je uitgebreider in de risicomatrix, waarin je ook de kans dat ze optreden, de impact en de manier waarop je met de risico's omgaat vermeldt. Tenslotte gaan we in op verschillende uitspraken die gevonden zijn vanuit de jurisprudentie.

# 2.Gebruik van de risicoanalyse

In dit hoofdstuk lees je wat de eerste stappen zijn om een risicoanalyse te maken.

## 2.1. 2.1 Quickscan

Deze risicoanalyse behelst een Quickscan aanpak die er voor zorgt dat op een pragmatische en effectieve manier de juiste risico's in kaart worden gebracht. Hiervoor gebruiken we het MAPGOOD model. MAPGOOD staat voor Mensen, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten. Dit zijn de verschillende invalshoeken om naar bedreigingen en risico's te kijken. Met behulp van de 7 componenten van het MAPGOOD model kan de Leverancier de risico's omtrent de ICT Prestatie categoriseren. MAPGOOD staat voor:

- Mens, de mensen die nodig zijn om het informatiesysteem te beheren en gebruiken.
- Apparatuur, de apparatuur die nodig is om het informatiesysteem te laten functioneren.
- Programmatuur, de programmatuur waaruit het informatiesysteem bestaat.
- Gegevens, de gegevens die door het systeem worden verwerkt.
- Organisatie, de organisatie die nodig is om het informatiesysteem te laten functioneren.
- Omgeving, de omgeving waarbinnen het informatiesysteem functioneert.
- Diensten, de externe diensten die nodig zijn om het systeem te laten functioneren

Belangrijk is dat voor ieder MAPGOOD-component afgewogen moet worden wat het risico is, hoe zwaar deze weegt, welke beheersmaatregel hierop kan volgen en waar het eigenaarschap ligt. Het gaat om de componenten in de hierna opgenomen tabel. Vervolgens geven we je een uitgebreide lijst met voorbeeldrisico's per component, conform het MAPGOOD model. Met behulp van de 7 componenten van het MAPGOOD model kan de Leverancier de risico's omtrent de ICT Prestatie categoriseren. De tabel is niet limitatief en niet alle risico's hoeven van toepassing te zijn op de ICT Prestatie. Van de Leverancier wordt verwacht dat hij bij een inschrijving of indiening van een offerte onderbouwt welke mitigerende maatregelen getroffen kunnen worden bij de aangegeven risico's.

## 2.2. Risico kans x impact

Een risicoanalyse is altijd het gevolg van de kans dat iets voorkomt X de impact dat iets heeft. Wij gebruiken hiervoor het volgende model:

Hoe groot is de impact:

| | | |
|---|---|---|
| Catastrofaal | 5 | Bedrijf gaat failliet of overname |
| Significant | 4 | Zelfde als gemiddeld, maar met negatieve publiciteit |
| Gemiddeld | 3 | Grote impact op kosten, meerkosten worden intern aangevuld. Geen invloed op de buitenwereld. |
| Laag | 2 | Impact kan eenvoudig gecompenseerd worden door interne verschuiving van middelen |
| Verwaarloosbaar | 1 | Geen verlies van tijd of geld |

Hoe groot is de kans:

| | | |
|---|---|---|
| Zekerheid | 5 | Nagenoeg zeker: 1 keer per jaar |
| Waarschijnlijk | 4 | Eens in de 2 jaar |
| Mogelijk | 3 | Eens in de 5 jaar |
| Onwaarschijnlijk | 2 | Eens in de 10 jaar |
| Minimaal | 1 | Enkel met bijzondere omstandigheden |

Kans x impact = mate van risico:

| **Kans x impact =** | **Niveau van risico** |
|---|---|
| 1-8 | Geen/verwaarloosbaar risico |
| 9-14 | Laag risico |
| 14-25 | Hoog risico ( beheersmaatregelen opstellen) |

**Tips**

- Voer altijd een risicoanalyse uit als het toeleveringsrisico en de invloed op het financiële resultaat hoog is (zie ook Kraljic in de Aedes Leidraden).
- Bepaal met je inkoopteam op welke risicosegmenten je een analyse uitvoert en gebruik hiervoor de voorbeelden in dit document als vertrekpunt.
- Gebruik de risicomatrix als een vast onderdeel van het inkoopplan.

## 2.3. Risicocomponenten op basis van MAPGOOD

| | Risicocomponent | Eigenaar | | | Kans | Impact | Mogelijke gevolgen | Beheersmaatregel |
|---|---|---|---|---|---|---|---|---|
| | | OG | Gedeeld | L | | | | |
| Mens | Wegvallen | | | | | | | |
| | Onopzettelijk foutief handelen | | | | | | | |
| | Opzettelijk foutief handelen | | | | | | | |
| Apparatuur | Spontaan technisch falen | | | | | | | |
| | Technisch falen door externe invloeden | | | | | | | |
| | Menselijk handelen/falen | | | | | | | |
| Programmatuur | Nalatig menselijk handelen | | | | | | | |
| | Onopzettelijk menselijk handelen | | | | | | | |
| | Opzettelijk menselijk handelen | | | | | | | |
| | Technische fouten/mankementen | | | | | | | |
| | Organisatorische fouten | | | | | | | |
| Gegevens | Via gegevensdragers (CD/DVD/ USB-sticks/ Harddisk/ Back-ups/ mobiele apparaten) | | | | | | | |
| | Via Cloud voorzieningen | | | | | | | |
| | Via apparatuur | | | | | | | |
| | Via programmatuur | | | | | | | |
| | Via personen | | | | | | | |
| | Gebruikersorganisatie | | | | | | | |
| | Beheerorganisatie | | | | | | | |
| | Ontwikkelingsorganisatie | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Omgeving | Huisvesting | | | | | | | |
| | Nutsvoorzieningen | | | | | | | |
| | Buitengebeuren | | | | | | | |
| Diensten | Diensten worden niet conform afspraak geleverd | | | | | | | |
| | Diensten dienstverlener tijdelijk niet beschikbaar | | | | | | | |
| | Diensten dienstverlener definitief niet meer te leveren | | | | | | | |

## 2.4. Voorbeelden verschillende risicocomponenten

| | Nr. | Risico | Eigenaar | | | Kans | Impact | Mogelijke gevolgen | Beheersmaatregel |
|---|---|---|---|---|---|---|---|---|---|
| | | | OG | Gedeeld | L | | | | |
| Mens | **Wegvallen:** | | | | | | | | |
| | 1 | Voorzienbaar (ontslag, vakantie) | | | | | | | |
| | 2 | Onvoorzienbaar (ziekten, overlijden, ongeval, staking) | | | | | | | |
| | **Onopzettelijk foutief handelen:** | | | | | | | | |
| | 3 | Onkunde, slordigheid | | | | | | | |
| | 4 | Foutieve procedures | | | | | | | |
| | 5 | Complexe foutgevoelige bediening | | | | | | | |
| | 6 | Onzorgvuldige omgang met wachtwoorden | | | | | | | |
| | 7 | Onvoldoende kennis/training | | | | | | | |
| | **Opzettelijk foutief handelen:** | | | | | | | | |
| | 8 | Niet werken volgens voorschriften/procedures | | | | | | | |
| | 9a | Diefstal | | | | | | | |
| | 9b | Fraude | | | | | | | |
| | 9c | Lekken van informatie | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 10 | Ongeautoriseerde toegang met account van medewerker met hogere autorisaties | | | | | | | |
| Apparatuur | **Spontaan technisch falen:** | | | | | | | | |
| | 11 | Veroudering/slijtage | | | | | | | |
| | 12 | Storing | | | | | | | |
| | 13 | Ontwerp/fabricage/ installatie/onderhoud fouten | | | | | | | |
| | **Technisch falen door externe invloeden:** | | | | | | | | |
| | 14 | Stroomuitval | | | | | | | |
| | 15 | Slechte klimaatbeheersing | | | | | | | |
| | 16 | Nalatig onderhoud door schoonmaak | | | | | | | |
| | 17 | Elektromagnetische straling | | | | | | | |
| | 18 | Elektrostatische lading | | | | | | | |
| | 19 | Natuurgeweld | | | | | | | |
| | 20 | Diefstal/schade | | | | | | | |
| | **Menselijk handelen/falen:** | | | | | | | | |
| | 21 | Installatiefout | | | | | | | |
| | 22 | Verkeerde instellingen | | | | | | | |
| | 23 | Bedieningsfouten | | | | | | | |
| | 24 | Opzettelijke aanpassingen/sabotage | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 25 | Beschadiging/vernieling | | | | | | | |
| | 26 | Verlies/diefstal (onder andere USB-sticks of andere gegevensdragers) | | | | | | | |
| | 27 | Verwijdering van onderdelen waardoor storingen ontstaan | | | | | | | |
| Programmatuur | **Nalatig menselijk handelen:** | | | | | | | | |
| | 28 | Ontwerp-, programmeer-, invoering, beheer/onderhoudsfouten | | | | | | | |
| | 29 | Introductie van virus en dergelijke door gebruik van niet gescreende programma's | | | | | | | |
| | 30 | Gebruik van de verkeerde versie van programmatuur | | | | | | | |
| | 31 | Slechte documentatie | | | | | | | |
| | **Onopzettelijk menselijk handelen:** | | | | | | | | |
| | 32 | Fouten door niet juist volgen van procedures | | | | | | | |
| | 33 | Installatie van malware en virussen door gebruik van onjuist/hoge autorisaties bijvoorbeeld gebruik admin-account tijdens browsen websites | | | | | | | |
| | **Opzettelijk menselijk handelen:** | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 34 | Manipulatie voor of na ingebruikname | | | | | | | |
| | 35 | (Ongeautoriseerde) functieverandering en/of toevoeging | | | | | | | |
| | 36 | Installatie van virussen, Trojaanse paarden en dergelijke | | | | | | | |
| | 37 | Kapen van autorisaties van collega's | | | | | | | |
| | 38 | Illegaal kopiëren van programmatuur | | | | | | | |
| | 39 | Oneigenlijk gebruik of privégebruik van bedrijfs-programmatuur | | | | | | | |
| | **Technische fouten/mankementen:** | | | | | | | | |
| | 40 | Fouten in code programmatuur die de werking verstoren | | | | | | | |
| | 41 | Achterdeuren in programmatuur voor (onbevoegde) toegang | | | | | | | |
| | 42 | Bugs/fouten in code die tot exploits kunnen leiden | | | | | | | |
| | **Organisatorische fouten:** | | | | | | | | |
| | 43 | Leverancier gaat failliet | | | | | | | |
| | 44 | Geen goede afspraken met leverancier | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Gegevens | **Via gegevensdragers (CD/DVD/ USB-sticks/ Harddisk/ Back-ups/ mobiele apparaten):** | | | | | | | | |
| | 45a | Diefstal/zoekraken | | | | | | | |
| | 45b | Lekken | | | | | | | |
| | 46 | Beschadiging door verkeerde behandeling | | | | | | | |
| | 47 | Niet overeenkomende bestandformaten | | | | | | | |
| | 48 | Foutieve of geen versleuteling | | | | | | | |
| | 49 | Foutieve of vervalste identificatie van ontvangers om aan gegevens te komen | | | | | | | |
| | **Via Cloud voorzieningen:** | | | | | | | | |
| | 50 | Ongeautoriseerde toegang door onbevoegden (hackers/hosters) | | | | | | | |
| | 51a | Ongeautoriseerde wijziging van gegevens (hacking) | | | | | | | |
| | 51b | Ongeautoriseerde verwijdering van gegevens (hacking) | | | | | | | |
| | **Via apparatuur:** | | | | | | | | |
| | 52 | Fysieke schrijf- of leesfouten | | | | | | | |
| | 53 | Onvoldoende toegangsbeperking tot apparatuur | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 54 | Fouten in interne geheugens | | | | | | | |
| | 55 | Aftappen van gegevens | | | | | | | |
| | **Via programmatuur:** | | | | | | | | |
| | 56 | Foutieve of gemanipuleerde programmatuur | | | | | | | |
| | 57 | Doorwerking van virussen/malware | | | | | | | |
| | 58 | Afbreken van verwerking | | | | | | | |
| | **Via personen:** | | | | | | | | |
| | 59a | (On)opzettelijke foutieve gegevensinvoer en -verandering van data | | | | | | | |
| | 59b | (On)opzettelijke foutieve gegevensverwijdering van data | | | | | | | |
| | 60 | Onbevoegde toegang door onbevoegden bijvoorbeeld hackers en dergelijke via malware | | | | | | | |
| | 61 | Onbevoegd kopiëren van gegevens | | | | | | | |
| | 62 | Meekijken over de schouder door onbevoegden | | | | | | | |
| | 63 | Onzorgvuldig vernietigen van gegevens bijvoorbeeld laten liggen op printer | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 64 | Niet toepassen clear screen/clear desk | | | | | | | |
| | 65 | Aftappen (draadloos) netwerk door onbevoegden (telewerk situaties) | | | | | | | |
| | 66 | Oneigenlijk gebruik van autorisaties | | | | | | | |
| | 67 | Toegang verschaffen tot gegevens door middel van identiteitsfraude of social engineering | | | | | | | |
| | **Gebruikersorganisatie:** | | | | | | | | |
| | 68 | Mismanagement | | | | | | | |
| | 69 | Gebrekkige toedeling taken, bevoegdheden en verantwoordelijkheden | | | | | | | |
| | 70 | Onduidelijke of ontbrekende gedragscodes | | | | | | | |
| | 71 | Afwezige, verouderde of onduidelijke handboeken/ systeemdocumentatie/ werkprocedures/ gebruiksinstructies | | | | | | | |
| | 72 | Onvoldoende interne controle | | | | | | | |
| | 73 | Onvoldoende toetsing op richtlijnen | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 74 | Onvoldoende of geen contractbeheer | | | | | | | |
| | 75 | Ontbrekende of onduidelijke SLA's | | | | | | | |
| | 76 | Gebrekkige doel/middelen beheersing | | | | | | | |
| | **Beheerorganisatie:** | | | | | | | | |
| | 77 | Gebrekkig beleid betreffende beheer | | | | | | | |
| | 78 | Onvoldoende kennis of capaciteit | | | | | | | |
| | 79 | Onvoldoende kwaliteitsborging | | | | | | | |
| | 80 | Onvoldoende beheer van systemen en middelen | | | | | | | |
| | **Ontwikkelingsorganisatie:** | | | | | | | | |
| | 81 | Slecht projectmanagement | | | | | | | |
| | 82 | Niet volgen van projectenkalender of PPM | | | | | | | |
| | 83 | Geen ontwikkelrichtlijnen en/of – procedures | | | | | | | |
| | 84 | Er worden geen methoden/technieken gebruikt | | | | | | | |
| | 85 | Gebrek aan planmatig werken | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Omgeving | **Huisvesting:** | | | | | | | | |
| | 86 | Ongeautoriseerde toegang tot gebouw(en) | | | | | | | |
| | 87 | Diefstal op werkplekken | | | | | | | |
| | 88 | Gebreken in ruimtes, waardoor kans op insluiping/inbraak | | | | | | | |
| | 89 | Onvoldoende fysieke voorzieningen om te vluchten of in te grijpen tijdens geweldsdreigingen /conflicten met klanten | | | | | | | |
| | **Nutsvoorzieningen:** | | | | | | | | |
| | 90 | Uitval van elektriciteit, water, telefoon | | | | | | | |
| | 91 | Wateroverlast door lekkage, bluswater | | | | | | | |
| | 92 | Uitval van licht-, klimaat- en/of sprinklerinstallatie | | | | | | | |
| | **Buitengebeuren:** | | | | | | | | |
| | 93 | Natuurgeweld (overstroming, blikseminslag, storm, aardbeving et cetera) | | | | | | | |
| | 94a | Overig geweld bijvoorbeeld oorlog, terrorisme, brandstichting en neerstortend vliegtuig | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 94b | Overig geweld bijvoorbeeld inbraak | | | | | | | |
| | 95 | Blokkade/staking | | | | | | | |
| | 96 | Onveilige, geblokkeerde, vluchtwegen bij brand | | | | | | | |
| **Diensten** | **Diensten worden niet conform afspraak geleverd:** | | | | | | | | |
| | 97 | Slecht opgeleid personeel | | | | | | | |
| | 98 | Groot personeelsverloop | | | | | | | |
| | 99 | Onvoldoende capaciteit in personeel | | | | | | | |
| | 100 | Valse verklaringen over certificeringen | | | | | | | |
| | 101 | Onvoldoende of geen kwaliteitsborging | | | | | | | |
| | 102 | Personeel voldoet niet aan eisen zoals een geldige VOG en getekende geheimhoudingsverklaring | | | | | | | |
| | 103 | Voert wanbeheer, slordigheden in beheersactiviteiten | | | | | | | |
| | 104 | Werkt niet conform ITIL of BiSL-principes | | | | | | | |
| | 105 | Maakt misbruik van toevertrouwde gegevens, applicaties en documentatie | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 106 | Houdt zich niet aan functiescheiding | | | | | | | |
| | 107 | Maakt gebruik van te zware autorisatie, niet functie gebonden | | | | | | | |
| | **Diensten dienstverlener tijdelijk niet beschikbaar:** | | | | | | | | |
| | 108 | Levert diensten niet conform overeenkomst | | | | | | | |
| | 109 | Onderbreking dienstverlening door overname dienstverlener | | | | | | | |
| | 110 | Kan diensten tijdelijk niet uitvoeren door zaken buiten de eigen controle bijvoorbeeld stakingen en dergelijke | | | | | | | |
| | 111 | Past verkeerde prioriteiten toe in klantbejegening | | | | | | | |
| | 112 | Levert onvoldoende capaciteit voor een goede dienstverlening | | | | | | | |
| | **Diensten dienstverlener definitief niet meer te leveren:** | | | | | | | | |
| | 113 | Een dienstverlener gaat failliet | | | | | | | |
| | 114 | Opzegging diensten door dienstverlener | | | | | | | |

De ACBIT is een set uniforme en gestandaardiseerde inkoopvoorwaarden die woningcorporaties en samenwerkingsverbanden kunnen gebruiken bij de inkoop van ICT-producten of -diensten. Een nadere specificatie van het toepassingsgebied van de ACBIT is beschreven in de toelichting bij de voorwaarden. In deze inleiding leggen we ook de link tussen ACBIT en het Aedes-programma Digitalisering.

## 2.5. ACBIT en de kwaliteitswijzer

Voor Opdrachtgevers is het van belang dat een in te kopen ICT-product of -dienst aansluit bij het bestaande IT omgeving als geheel. Om deze aansluiting te realiseren is het veelal nodig dat de ICT Prestatie voldoet aan normen en standaarden, bijvoorbeeld op gebied van Interoperabiliteit of beveiliging. In deze kwaliteitswijzer staan voorbeelden van belangrijke kwaliteitsgebieden, die in algemene zin voor corporaties geschikt zijn. De onderwerpen die in dit document zijn beschreven, sluiten aan op de ACBIT en de bijbehorende overeenkomstengenerator. Dankzij een koppeling tussen de ACBIT en de kwaliteitswijzer is geborgd dat ICT Prestatie, door opdrachtgever en opdrachtnemer, voldoende in ogenschouw worden genomen.

In de corporatiesector speelt een aantal ontwikkelingen die werken aan ICT kwaliteit noodzakelijk maken. Het convenant verbeteren informatievoorziening, de verduurzaming van de corporatievoorraad, het digitaliseren van de dienstverlening aan huurders, ketenintegratie met toeleveranciers en strengere regelgeving rond privacy. ICT-ontwikkelingen volgen elkaar snel op. Daarom is dit de eerste versie van de kwaliteitswijzer. We streven er naar deze verder aan te vullen.

In de ACBIT is de kwaliteitswijzer als volgt gedefinieerd:

*'Het door de Aedes gepubliceerde en van tijd tot tijd bijgewerkte document met een gebundelde verzameling van normen en standaarden voor ICT-producten en -diensten.'*

## 2.6. De basis op orde

Om de ACBIT te kunnen gebruiken is het belangrijk om de basis op orde te hebben. Zoals bijvoorbeeld Opdrachtgeverschap en Inkoop. In de Aedes Governancecode is het volgende opgenomen: Bestuur en RvC hebben een visie op opdrachtgeverschap en het beleid van aanbestedingen. Dit beleid onderschrijft de beginselen van aanbesteden; namelijk gelijke behandeling, objectiviteit, transparantie en proportionaliteit (artikel 5.3). In het stappenplan van de ACBIT gaan we dieper op deze onderwerpen in.

## 2.7. Aedes-programma Digitalisering

Digitalisering verandert de wereld om ons heen en kan een bijdrage leveren aan efficiënter werken. Dienstverlening aan huurders en samenwerking met ketenpartners wordt steeds meer digitaal. Ook transformeert digitalisering de bedrijfsvoering van corporaties. Aedes werkt samen met corporaties aan randvoorwaarden om digitalisering voor hen makkelijker te maken.

Het Aedes-programma Digitalisering bestaat uit de volgende projecten:

- Professionalisering van datastandaarden in de sector. Het gaat hierbij om afspraken tussen corporaties en ketenpartners over eigenaarschap, vastlegging en uitwisseling van data. Dit moet ervoor zorgen dat corporaties data van hoge kwaliteit makkelijk beschikbaar krijgen.
- Sectorale digitaliseringsvisie en -strategie, met afspraken over de belangrijkste doelstellingen om de sector te digitaliseren in de komende jaren (tot 2030).
- De belangrijkste werkprocessen binnen een woningcorporatie worden uitgewerkt in het processenboek. Een goed beschreven proces bespaart tijd en geld. Het helpt om processen

efficiënter uit te voeren en beter te digitaliseren. Ook draagt het bij aan betere sturing en vermindering van risico's.
- Een gestandaardiseerd grootboekschema maakt het eenvoudiger om financiële gegevens uit te wisselen en te analyseren. Dit staat bekend als het Referentie Grootboekschema (RGS).
- Aanleverketen voor verantwoordingsinformatie. De methodiek hiervoor is Standard Business Reporting, en voor de corporatiesector zet SBR-wonen zich daarvoor in.
- We helpen corporaties bij het ontwikkelen van de competenties die ze nodig hebben om hun datakwaliteit voor de sturingsinformatie en dienstverlening te verbeteren.
- De pilot Digitale inkomenstoets stelt huurders in staat om via DigiD hun inkomensgegevens te delen met corporaties, zodat die daarmee de verplichte inkomenstoets uit kunnen voeren.

In het stappenplan van de ACBIT gaan we dieper op deze onderwerpen in.

## 2.8. Leeswijzer

Dit document beschrijft allereerst hoe je de kwaliteitswijzer kunt toepassen. Vervolgens gaan we in op welke normen en standaarden zijn opgenomen in de kwaliteitswijzer, en welke (nog) niet. Tenslotte komen de verschillende kwaliteitsgebieden aan bod die het vertrekpunt zijn van de ACBIT. In dit document worden, daar waar mogelijk, bij de verschillende kwaliteitsgebieden het doel, indien van toepassing wet- en regelgeving en tips over mogelijke standaarden of normen beschreven.

# 3. GEBRUIK VAN DE KWALITEITSWIJZER

## 3.1. Aanbevelingen bij gebruik van kwaliteitswijzer

De kwaliteitswijzer is in de eerste plaats bedoeld als vangnet. Bij het ontbreken van afwijkende afspraken moet de Leverancier ervoor zorgen dat de ICT Prestatie voldoet aan de daarvoor relevante normen en standaarden zoals is opgenomen in de ACBIT (ACBIT-artikel 6.1 sub i).

Om een zo passend mogelijk aanbod van leveranciers te krijgen, is het echter aan te bevelen tijdens het voorbereidingsproces van een inkooptraject de kwaliteitsgebieden nader te bekijken en te specificeren. Hiervoor kunnen 5 aanbevelingen worden gedaan.

1. *Stel vast wat je nodig hebt*
   De basis van de ACBIT wordt gevormd door de overeenkomstengenerator. Dit is als het ware de spil waar alles samen komt. Voor het bepalen van de totale leveringsomvang verwijzen wij naar het Aedes inkoopproces en het stappenplan. In het voortraject bepaal je wat je nodig hebt, daarna volgt de aanbesteding en vervolgens maak je de overeenkomst. Gebruik hiervoor de overeenkomstengenerator. We raden van harte aan om zo veel mogelijk gebruik te maken van de binnen de sector gebruikelijke 'standaarden', indien dat niet mogelijk is van 'halffabrikaten' en anders van maatwerk. Zorg er tenslotte voor dat je bekend bent met de artikelen die opgenomen zijn in de ACBIT. Hiervoor kun je de toelichting op het ACBIT lezen.

2. *Geef relevante kwaliteitsgebieden in de opdrachtdocumentatie nader invulling*
   Nader invulling te geven aan relevante kwaliteitsgebieden, zoals vraagspecificatie en overeenkomst, maakt het voor zowel opdrachtgever als leverancier duidelijk aan welke normen (delen van) de ICT Prestatie precies moet voldoen. Bovendien worden onnodige kosten vermeden door implementatie van (delen van) normen of standaarden waaraan geen behoefte is. Nadere specificatie is met name van belang voor toepassingsafhankelijke normen, zoals Interoperabiliteit (toe passen standaarden hangen af van het toepassingsgebied van de ICT Prestatie), Informatiebeveiliging en Privacy (beveiligingsniveau is onder andere afhankelijk van gevoeligheid van met de ICT Prestatie verwerkte gegevens).

3. *Betrek (domein)experts bij het vaststellen van de relevantie van kwaliteitsgebieden*
   Deze aanbeveling ligt in het verlengde van de vorige. Het nader invullen van aantal kwaliteitsgebieden vereist veelal specialistische kennis en ervaring. Dit zal bijvoorbeeld vaak gelden voor normen ten aanzien van Architectuur, Interoperabiliteit, Informatiebeveiliging en Archivering.

4. *Neem relevante kwaliteitsgebieden expliciet op in de opdrachtdocumentatie*
   Hierdoor is, in gevallen waar als onderdeel van de opdracht onderhoud wordt gepleegd, het bijwerken naar nieuwe versies van normen of standaarden gewaarborgd (ACBIT-artikel 8.10 sub ii).

5. *Gebruik de overeenkomstengenerator om een (concept)overeenkomst te generen*
   In de overeenkomstengenerator is ruimte om met de ACBIT en de Corporatie ICT-kwaliteitsgebieden als basis een overeenkomst te genereren die nadere of afwijkende afspraken omvat. De overeenkomstengenerator is te vinden op aedes.acbit.nl.

## 3.2. Reikwijdte kwaliteitswijzer

De kwaliteitswijzer betreffen normen en standaarden waaraan voldaan kan worden. We maken een onderscheid in verplichtingen en keuzemogelijkheden.

De *verplichting* kan volgen uit:

1. een wettelijk kader en/of
2. opname op de lijst van open standaarden (pas-toe-of-leg-uit) en/of
3. generieke (internationale) standaarden voor ontwikkeling en beheer van ICT producten en diensten.

*Keuzemogelijkheden* komen voort uit:

1. een breed erkende woningcorporatie standaard en/of
2. een standaard die wordt gebruikt binnen specifieke ketens waarin corporaties werkzaam zijn (denk aan: bouw-, installatie- en vastgoedsector).

Verplichte normen zijn, bijvoorbeeld vanuit een wettelijk kader, vastgesteld. Standaarden of versies van standaarden die nog in ontwikkeling zijn (nog) geen onderdeel zijn van de kwaliteitswijzer. Het vaststellingsproces kan per kwaliteitsnorm verschillen. Dit is mede afhankelijk van de beheerder en governancestructuur bij de betreffende norm. Voor wettelijke normen geldt de wetgever als vaststeller. Landelijk vastgestelde open standaarden worden vastgesteld onder regie van het Forum Standaardisatie. Generieke ICT standaarden worden vastgesteld door standaardisatie instituten als ISO en W3C. Specifieke woningcorporatie standaarden worden onder regie van Aedes en het bestuur van CorpoNet vastgesteld. In alle gevallen is een proces ingericht waarbij woningcorporaties en leveranciers nauw betrokken zijn, en mede bepalen hoe de norm of standaard eruit gaat zien.

### 3.2.1. Kwaliteitsgebieden

Verschillende kwaliteitsgebieden zijn een onderdeel van de ACBIT. In hoofdstuk 3 gaan we daar, per onderdeel dieper op in.

- Architectuur
- Interoperabiliteit
- Informatiebeveiliging en privacy
- Dataportabiliteit
- Toegankelijkheid
- Archivering
- Infrastructuur
- Documentatie

De door de Opdrachtgever gekozen kwaliteitsgebieden uit de kwaliteitswijzer zijn van toepassing als de ACBIT van toepassing is verklaard. Dit geldt zowel in de situatie dat een overeenkomst wordt gesloten waarop de ACBIT van toepassing is verklaard, als wanneer een opdrachtgever tijdens een uitvraag (bijvoorbeeld tijdens het inkoopproces) aangeeft dat de ACBIT van toepassing is.

In ACBIT-artikel 6.1(i) is beschreven dat het voldoen aan de gekozen normen uit de kwaliteitswijzer onderdeel is van het ‘Overeengekomen gebruik’. Hieruit volgt dat Leverancier (maar ook de Opdrachtgever) geacht wordt bekend te zijn met (de inhoud van) de kwaliteitswijzer.

Concreet betekent artikel 6.1 dat de ICT Prestatie ('de te leveren goederen en diensten') moet voldoen aan de gekozen normen uit de kwaliteitswijzer. Hierop zijn echter 2 beperkingen van toepassing.

1. Bereik: er hoeft alleen te worden voldaan aan de opgenomen interoperabiliteitseisen, normen en standaarden voor zover die relevant zijn voor de functie of gelden voor het werkingsgebied van de ICT Prestatie.
2. Tijd: er hoeft alleen te worden voldaan aan die interoperabiliteitseisen, normen en standaarden die tijdens het sluiten van de Overeenkomst voorgeschreven waren. Hoewel het voldoen aan bij nieuwe versies onderdeel kan zijn van afspraken over Onderhoud, zie hieronder.

De in de ACBIT voorgeschreven normen en standaarden zijn **minimumeisen**. ACBIT-artikel 6.1 ii creëert voor Opdrachtgevers dan ook de mogelijkheid om van Leveranciers te vragen te voldoen aan aanvullende normen en standaarden - bijvoorbeeld de verplichte implementatie van een standaard. Maar de gekozen normen uit de kwaliteitswijzer hebben, op het moment van schrijven, slechts een aanbevolen karakter. Met andere woorden: Opdrachtgevers maken zelf de keuze welke kwaliteitsgebieden van toepassing zijn. Daarom moet de Opdrachtgever wel expliciet in de vraagspecificatie om deze normen worden gevraagd en vastgelegd in de Overeenkomst.

ACBIT-artikelen 6.2 t/m 6.5 zien toe op het uitvoeren van (preventieve) testen van de ICT Prestatie ten aanzien van de gekozen normen uit de kwaliteitswijzer. Artikel 6.4 bepaalt dat tijdens de Acceptatieprocedure getoetst wordt of voldaan is aan de krachtens 6.1 toe te passen normen. Bij individuele normen binnen kwaliteitswijzer moet worden aangegeven welke testvoorzieningen beschikbaar en te gebruiken zijn.

## 3.3. Nieuwe versies en updates

Normen en standaarden kunnen tijdens de looptijd van een Overeenkomst veranderen. Van veel normen verschijnen immers regelmatig nieuwe of bijgewerkte versies. Om Interoperabiliteit en het voldoen aan wetgeving tijdens de contractperiode te garanderen, is het noodzakelijk dat deze nieuwe versies binnen een redelijke termijn worden geïmplementeerd. Ook dit is in de ACBIT vastgelegd.

Wat die redelijke termijn is, is niet in algemene zin te zeggen. Voor de verplichte normen (bijvoorbeeld vanuit wetgeving), zijn aanpassingen echter vrijwel altijd ruim van tevoren te voorzien. Bij vaststelling van (aangepaste) normen is bovendien vaak sprake van een overgangsperiode, zoals de periode tussen vaststelling en het daadwerkelijk ingaan.

Om implementatie van nieuwe (versies van) normen en standaarden tijdens de looptijd van de overeenkomst te ondersteunen, is in ACBIT-artikel 8.10 sub iii bepaald dat het implementeren van nieuwe versies van normen en standaarden onderdeel is van het Onderhoud dat Leverancier uitvoert. Deze verplichting wordt beperkt tot die normen en standaarden waarvoor implementatie in de Overeenkomst expliciet en verplichtend is benoemd. Tegenover deze verplichting kan een vergoeding staan. ACBIT-artikel 8.1 nodigt Leverancier en Opdrachtgever uit hierover in de Overeenkomst afspraken vast te leggen.

# 4. KWALITEITSGEBIEDEN

## 4.1. Architectuur

ICT-architectuur is een verzameling van regels en standaarden op basis waarvan systemen worden ontwikkeld.

### 4.1.1. Doel

Woningcorporaties hebben een breed taken- en dienstenpakket. Gevolg is dat er een landschap van verschillende informatiesystemen nodig is om goed invulling te kunnen geven aan die taken en diensten. Ook wel de IT-omgeving of Architectuur genoemd. Er is behoefte aan inzicht en overzicht ten aanzien van dat landschap en de processen om goed te kunnen sturen en organiseren. De Leverancier moet aangeven hoe de aangeboden ICT-dienst past binnen dit landschap. Ook dit is vastgelegd in de ACBIT. Daarnaast wordt van een leverancier verwacht dat de beheerprocessen zodanig zijn ingericht dat ze goed aansluiten bij interne beheerprocessen van de woningcorporatie.

### 4.1.2. Wet- en regelgeving

Uitgangspunt is dat de corporatie de ICT Prestatie heeft ingericht conform alle geldende wet- en regelgeving.

- Woonruimtebemiddelingssysteem
  Denk daarbij aan zaken als huurprijsgrenzen, blokkadelijsten en huur- en inkomenstabellen. Indien van toepassing zal een jaarlijkse aanpassing van het systeem nodig zijn.
- AVG en privacy
  Met de inwerkingtreding van de AVG in mei 2018 is privacy een nog belangrijker onderwerp geworden. Beperkte ICT kwaliteit is vaak het gevolg van onduidelijke afspraken over opslag en eigenaarschap van data. Maak hier eenduidige afspraken over en bewaar privacygevoelige gegevens alleen op gevalideerde locaties. Zo voldoe je aan de wetgeving en verhoog je de ICT prestatie.

### 4.1.3. Tip

Vraag aan de leverancier de in werking zijnde bedrijfsprocessen voor de ICT dienstverlening te overleggen. Deze dienen - bij voorkeur - gestoeld te zijn op algemeen toegepaste modellen zoals ITIL, ISM, ASL en BISL.

## 4.2. Interoperabiliteit

Interoperabiliteit gaat over het uitwisselen van data tussen systemen.

### 4.2.1. Doel

Woningcorporaties maken gebruik van systemen van meerdere Leveranciers, willen voor een efficiënte uitvoering en dienstverlening informatie delen, en werken in ketens samen met andere (overheids-) partijen. Gevolg is dat woningcorporaties in staat moeten zijn om gegevens tussen verschillende systemen uit te wisselen. Goede, veilige en betrouwbare koppelingen zijn hiervoor noodzakelijk. Het gebruik van open standaarden voor Interoperabiliteit zorgt voor inpasbaarheid van ICT Prestaties binnen de IT omgeving van woningcorporaties.

Dit leidt voor woningcorporaties tot meer samenhang in de IT-omgeving, grotere flexibiliteit in informatievoorziening en meer keuzevrijheid ten aanzien van software. Tevens zorgt het gebruik van standaarden voor het voorkomen van maatwerkkoppelingen en extra werkzaamheden die daaraan verbonden zijn.

### 4.2.2. Tips

- Er is een lijst met aanbevolen standaarden van het Forum Standaardisatie: forumstandaardisatie.nl/open-standaarden/lijst/aanbevolen. Deze standaarden zijn niet verplicht, maar worden geadviseerd om te gebruiken voor een betreffend functioneel werkingsgebied. Opdrachtgevers wordt aangeraden om in hun vraagspecificatie heel duidelijk aan te geven welke van die aanbevolen standaarden verplicht worden gesteld (dit is conform ACBIT artikel 6.1 ii).
- Monitoring API: een standaard om energieprestaties van gebouwen te monitoren. Zie github.com/Stroomversnelling?tab=repositories, monitoringnorm.nl.

## 4.3. Informatiebeveiliging en privacy

Informatiebeveiliging is het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Hieronder valt bijvoorbeeld het onderhouden en controleren van een samenhangend pakket van bijbehorende beveiligingsmaatregelen.

### 4.3.1. Doel

Woningcorporaties verwerken veel informatie, waarvan een deel zeer (privacy)gevoelig is en extra beschermd dient te worden. Voor een groot deel van die informatieverwerking wordt gebruik gemaakt van ICT-producten en -diensten van derden. Met hen moeten goede afspraken worden gemaakt over beveiliging en het waarborgen van privacy. Betrouwbare informatiesystemen dragen bij aan het verlagen van risico's en vergroten van de weerbaarheid van de bedrijfsvoeringsprocessen van de woningcorporatie. Woningcorporaties verwerken veel persoonsgegevens. Vaak is het daarom nodig met leveranciers een verwerkersovereenkomst af te sluiten.

### 4.3.2. Tips

- Ten aanzien van informatiebeveiliging zijn er internationale en landelijk vastgestelde normen en standaarden. De Baseline Informatiebeveiliging Corporaties (BIC) is het normenkader dat de beschikbaarheid, integriteit en exclusiviteit van woningcorporatie informatie-(systemen) bevordert. Deze Baseline is een richtlijn die een totaalpakket aan informatiebeveiligingsrichtlijnen en -maatregelen omvat die voor iedere woningcorporatie geldt.
- In 2019 is de BIC aangevuld met de Bic Building Blocks (BBB). Die zijn ontwikkeld om de implementatie van de Baseline Informatiebeveiliging Corporaties (BIC) te vereenvoudigen. De BBB is een set ondersteunende documenten die corporaties kunnen helpen bij de praktische implementatie van de BIC.
- Naast de BIC zijn ook de beveiligingsstandaarden van toepassing die vallen binnen de open standaarden (zie 3.2 Interoperabiliteit).

## 4.4. Dataportabiliteit

Dataportabiliteit wordt ook wel gegevensoverdracht genoemd.

### 4.4.1. Doel

Woningcorporaties beheren veel data. Deze data zijn nodig om taken en diensten te verrichten. Vaak liggen deze data opgeslagen in ICT Prestaties van Leveranciers, waar ook verwerking en creatie van data kan plaatsvinden. Het doel van Dataportabiliteit is zorgen dat de Opdrachtgever altijd toegang heeft tot de eigen data en deze betekenisvol kan overzetten naar andere systemen. Dataportabiliteit is de mogelijkheid eigen gegevens geautomatiseerd uit een informatiesysteem naar een ander systeem te kunnen verhuizen. Daar waar Interoperabiliteit gaat over samenwerking en koppelingen tussen systemen, gaat Dataportabiliteit over het eruit halen van gegevens (exporteren) en zonder verlies van betekenis overzetten (migreren/importeren) naar een ander systeem of platform. Dataportabiliteit is noodzakelijk voor het op lange termijn beschikbaar houden van ICT functionaliteiten, meer regie en bescherming van eigen gegevens, en het makkelijker kunnen wisselen van leverancier en/of systeem.

### 4.4.2. Wet- en regelgeving

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. In de AVG is Dataportabiliteit ook opgenomen. Artikel 20 van de AVG betreft de verplichting tot het waarborgen van het 'Recht op overdraagbaarheid van gegevens' oftewel 'gegevensoverdraagbaarheid'.

### 4.4.3. Tips

Dataportabiliteit heeft zowel betrekking op de inhoud (waarden) van de data als op de bijbehorende metadata over de structuur en betekenis van die gegevens. Voor het geautomatiseerd omzetten hiervan dient dit in een gangbaar formaat te gebeuren.

De metadata omvatten tenminste:

- de beschrijving van de betekenis van entiteiten, relaties, attributen, datatype en waardenbereik;
- het technische formaat;
- de beschrijving van betekenis en relaties tussen gegevens;
- het formaat waarin data kan worden geëxporteerd/geïmporteerd;
- welke gegevens en metadata wel en niet worden meegenomen en het formaat waarin dat plaatsvindt;
- de beschrijving van de import en exportfunctionaliteit die het softwareproduct ondersteunt;
- de data die niet in de import en export meegenomen wordt omdat deze geen eigendom is van Opdrachtgever;
- opgave van de technische formaten die voor dataportabiliteit gebruikt worden.

## 4.5. Toegankelijkheid

Digitale toegankelijkheid is het gebruik maken van de mogelijkheden die internet, computers, apps en smartphones ons bieden.

### 4.5.1. Doel

In Nederland willen we dat openbare voorzieningen toegankelijk zijn voor alle burgers. Niet alleen gebouwen en bijvoorbeeld het openbaar vervoer, maar ook overheidswebsites.

In de Aedes Governancecode hebben wij vastgelegd dat onder andere het jaarverslag en de interne gedragscode openbaar op de website van de corporatie moet worden gedeeld. Daarom is digitale toegankelijkheid ook voor corporaties belangrijk.

#### 4.5.2. Archivering

Het archiveren van digitale informatie en documenten op een gestructureerde wijze, met een goed ingericht digitaal archief en/of systeem.

#### 4.5.3. Doel

Archivering heeft tot doel het zorgdragen dat gegevens duurzaam beschikbaar blijven, zodat het handelen van woningcorporaties (publiek) verantwoord kan worden. Hiertoe dienen archiefbescheiden in geordende en toegankelijke staat te zijn. Voor een goede vindbaarheid en archivering van informatie en uitwisseling van informatie met ketenpartijen, is metadatering van (digitale) informatie noodzakelijk. Metadata geven informatie over dossiers van een woningcorporatie. In metadata is informatie vastgelegd over de inhoud, context, structuur, vorm en het beheer van dossiers door de tijd heen.

#### 4.5.4. Wet- en regelgeving

Woningcorporaties vallen niet onder de Archiefwet. Zij mogen zelf kaders, beleid en regels opstellen voor het beheer van digitale documenten. Daarbij wordt vaak wel rekening gehouden met de strekking van de Nederlandse archiefwet en -regelgeving. Ook kan men de lijn aanhouden die voortkomt uit andere (informatie)wetgeving, bijvoorbeeld voor het bepalen van bewaartermijnen.

#### 4.5.5. Tip

Maak afspraken met Leveranciers over aantoonbare voorzieningen om aan de bewaartermijnen te voldoen. Soms wordt in plaats van bewaartermijn ook wel gesproken van opslagtermijn of de data-retentietermijn.

## 4.6. Infrastructuur

Infrastructuur is een combinatie van hardware, software, netwerken en faciliteiten (inclusief gerelateerde apparatuur) die worden gebruikt om IT-services te ontwikkelen, testen, leveren, bewaken, controleren of ondersteunen. (Semi-)Overheidsbrede voorzieningen bieden een gemeenschappelijke basis om de dienstverlening te verbeteren.

#### 4.6.1. Doel

De sector kent een groot aantal stakeholders waaronder het ministerie van BZK, het Waarborgfonds Sociale Woningbouw en de Autoriteit woningcorporaties. Daarnaast is er contact met gemeenten, het CBS en de Belastingdienst. Ook met hen wordt informatie uitgewisseld. Deze organisaties werken steeds meer digitaal. Een goed beheer van woningen is mede afhankelijk van een goed beheer van informatie. De volledigheid en de kwaliteit van data zijn daarbij bepalend. Efficiënt en effectief samenwerken met de eerder vermelde partijen én Leveranciers, waarbij veel data worden uitgewisseld, vraagt om steeds verdergaande digitalisering. Het doel is te borgen dat de gemeenschappelijke voorzieningen (her)gebruikt worden en dat er makkelijker informatie tussen (semi-)overheidsdiensten onderling, en met bedrijven en burgers kan worden uitgewisseld.

### 4.6.2. Tips

- Het referentiegrootboekschema (RGS) is een standaardgrootboekschema dat landelijk is afgesproken in een publiek-private samenwerking tussen onder andere accountantskoepel NBA, CBS, Belastingdienst, banken en softwareleveranciers. RGS maakt onderdeel uit van het Standard Business Reporting programma (SBR) van de overheid. Corporaties kunnen RGS gebruiken om hun boekhouding (deels) te standaardiseren. Uit deze gestandaardiseerde boekhouding kunnen vervolgens automatisch financiële rapporten worden gegenereerd en via SBR verzonden naar toezichthouders.
- De koppeling tussen SBR en RGS heet de `RGS taxonomie'. Om van RGS gebruik te kunnen maken, is het nodig dat uw software RGS en SBR voldoende ondersteunt.
- Voor asbestinventaristies wordt gebruik gemaakt van het Landelijk Asbest Volg Systeem (LAVS). Het systeem wordt beheerd door Rijkswaterstaat
- Het Kadaster beheert de basisregistraties BAG (Basisregistratie Adressen en Gebouwen) en BRK (Basisregistratie Kadaster). Corporaties maken gebruik van die voorzieningen om inzicht te houden in hun eigen vastgoedbezit
- Energielabels worden vastgelegd in de landelijke database EP-online van de Rijksdienst voor Ondernemend Nederland (RVO)

## 4.7. Documentatie

Documentatie is het informatiesysteem ten behoeve van de informatievoorziening. Zonder documentatie is een efficiënte en effectieve bedrijfsvoering niet realiseerbaar.

### 4.7.1. Doel

Goede documentatie is noodzakelijk om een ICT Prestatie optimaal te implementeren, in te passen in de IT omgeving, te gebruiken binnen een bedrijfsproces, keten en/of in dienstverlening en te beheren en te onderhouden. ACBIT artikel 11.1 geeft aan welke inhoudelijke eisen gelden ten aanzien van documentatie.

### 4.7.2. Tips

Maak met Leverancier afspraken over:

- Lokaliseerbaarheid: het moet duidelijk zijn waar welk onderwerp te vinden is.
- Consistentie: de documentatie mag geen innerlijke tegenstrijdigheden bevatten.
- Onderhoudbaarheid: de documentatie moeten op economisch verantwoorde wijze te onderhouden zijn.
- Juistheid: de documentatie moet correct zijn.
- Actualiteit: de status van de documentatie moet parallel lopen met de status van het informatiesysteem.
- Volledigheid: in de documentatie mogen geen 'witte vlekken' aanwezig zijn.
- Nauwkeurigheid: de documentatie moet over een op het gebruiksdoel afgestemde nauwkeurigheid bezitten.
- Controleerbaarheid: de documentatie moet met gemak op juistheid en volledigheid te controleren zijn.