ACBIT Risicoanalyse

Onderdeel van de ACBIT, Algemene Corporatie Inkoopvoorwaarden bij IT

Mei 2024

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 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, maar daar vervolgens ook wat mee doen door deze informatie te vertalen in het aanbod en de risicoanalyse. 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. Ook is er een toolbox voor het inkopen van ICT beheer. De inkooptoolbox ICT beheer kun je vinden in de community OPDRACHTGEVERSCHAP .

De inkooptoolbox sluit aan bij het Aedes inkoopproces en de ACBIT. In de inkooptoolbox voor ICT beheer zit o.a een strategiedocument (welke keuzes maakt jouw corporatie), een inkoopplan (verzamelen van informatie om een specificatie op te stellen), offerteaanvraag en beoordelingsdocumenten.

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. 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.

1.4. Leeswijzer

Dit document beschrijft allereerst hoe de risicoanalyse is opgebouwd. Daarna 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.

2.Gebruik van de risicoanalyse

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

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							