Audit Alert
Keteninformatisering

NOREA
de beroepsorganisatie van IT-auditors

NOREA, de beroepsorganisatie van IT-auditors
Bezoekadres:
Antonio Vivaldistraat 2-8
1083 HP Amsterdam

Postadres:
Postbus 7984
1008 AD Amsterdam
norea@norea.nl
www.norea.nl
tel +31 (0)20 3010380

Werkgroep Ketenauditing
Drs. B. (Bart) J. van Staveren RE, UWV - voorzitter
Drs. M. (Michael) Bosch RE, Ministerie van Binnenlandse zaken en Koninkrijksrelaties
A. (Adri) J.M. de Bruijn RE RA, PwC Advisory
Dr. R. (Rene) P.M. Matthijsse RE, KPMG Management Consulting
R. (Ruud) J. Mollema RE RA, PBLQ
R. (Ruurd) Smildiger RE, Auditdienst Rijk
Drs. R. (Reza) Torabkhani RE, AlignNet
Drs. M. (Marc) M.J.M. Welters RE RA, Ernst & Young Accountants

Inhoudsopgave

Datum	:	21 maart 2013
Betreft	:	NOREA Audit Alert Keteninformatisering

Geachte bestuurder,

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) constateert in haar rapport iOverheid (2011) dat sprake is van een vernetwerkte, i.e. het gezamenlijk gebruik en beheer van informatie in een netwerk van actoren, en gedigitaliseerde overheid in Nederland.

De NOREA, de beroepsorganisatie van IT-auditors (RE´s), houdt zich in de werkgroep Ketenauditing al lange tijd bezig met de gevolgen van deze dominante ontwikkeling: keteninformatisering. Door middel van deze Alert wil zij u op de hoogte brengen van de uitkomsten van haar onderzoek. In de bijlage gaan wij in op een aantal ontwikkelingen en bedreigingen in ketens. Als voorbeelden zijn grotendeels ketens vanuit de overheid genomen, maar deze zijn eenvoudig te projecteren op ketens in de zorg, betalingsverkeer, luchtvaart en industrie. Een kenmerk van deze informatieketens is dat de processen over de organisaties heen worden uitgevoerd en dat de ketenpartners hun organisatie-inrichting wederzijds kunnen beïnvloeden.

Deze informatieketens zijn effectief, maar naar onze mening bepaald niet zonder risico's. Daarbij hebben wij vanuit de ervaringen van onze IT-auditors sterk de indruk dat risico- en beveiligingsspecialisten hun management te weinig informeren over de omvang van de risico's van de keteninformatisering. Het gevolg is dat bestuurders veelal ten onrechte het idee hebben dat hun organisatie weinig risico's loopt. In de praktijk komen regelmatig incidenten voor met gevolgen voor een hele keten.

Aan de andere kant zien wij betrokken bestuurders die de risico's wel degelijk onderkennen en bespreken. Zij lijken echter niet in staat hun organisaties in de context van een keten effectief aan te sturen dan wel adequate maatregelen te treffen, zoals met behulp van kaders en voorschriften.

Na een langdurig onderzoek naar en evaluatie van de problematiek rondom informatieketens binnen de overheid concludeert de NOREA-werkgroep Ketenauditing dat het bij de toekomst van de digitale overheid in Nederland gaat om het hebben en houden van vertrouwen in de werking van informatieketens. Dit wordt in de volgende zes aandachtspunten uiteengezet:

1) Informatieketens werken op basis van vertrouwen in de informatie die binnen de keten wordt verwerkt. Dat vertrouwen in elkaar probeert men te staven door het gebruik van unieke nummers, zoals het Burgerservicenummer en authentieke registers.
2) Er zijn helaas (langdurige) uitvalverschijnselen en andere haarscheurtjes in de informatieketens die het vertrouwen aantasten (zie de voorbeelden in de bijlage). IT-auditors hebben geconstateerd dat lijnmanagers de continuïteits- en beveiligingsrisico's met betrekking tot de informatieketens vanuit hun organisatie te laag inschatten.
3) Er is te weinig sprake van gefundeerd vertrouwen in informatieketens die op een bepaald moment onder normale omstandigheden functioneren. Het is door gebrek aan documentatie en afspraken vaak onduidelijk of er adequate maatregelen in de gehele keten getroffen zijn die ervoor zorgen dat zij blijvend goed functioneert. Daarmee is er ook geen zicht op de risico's die gelopen worden bij het optreden van problemen.
4) De oplossingsrichting ligt in het borgen van vertrouwen door het versterken van de fundamenten door middel van zekerheden (techniek, standaarden, afspraken, toezicht en sturing) en transparantie daarover. Deze worden in de bijlage bij deze alert verder uitgewerkt.

5) Dit vertrouwen is van groot belang voor de bestuurders van departementen en uitvoeringsorganisaties omdat de digitale overheid ‘zwarte zwanen’ in zich bergt, i.e. risico’s waarvan men zich niet bewust is. Een op audit en onderzoek gefundeerd vertrouwen verkleint de kans op ‘zwarte zwanen’, want “meten doet weten”.
6) Bestuurders moeten om deze reden de verantwoordelijkheid nemen om transparantie over de fundamenten in de keten te verschaffen. Dit kan niet beter dan door de kwaliteit van de techniek, standaarden, afspraken, toezicht en sturing in ketens objectief te laten beoordelen en verbeteringen te laten volgen.

Audit en onderzoek vormen in het moderne denken het sluitstuk van Goed Bestuur. Enerzijds voor de interne beheersing, want het besturen van een organisatie is ook het voortdurend toetsen of de risico’s worden beheerst en de procedures worden nageleefd. Anderzijds voor de verantwoording naar buiten, immers overheidsketens en –netwerken zijn voor en van ons allemaal. Het afleggen van verantwoording daarover behoort deel uit te maken van Goed Bestuur. Audit en onderzoek kunnen gericht zijn op de samenwerking tussen de organisaties op drie niveaus:

- het strategische niveau: hoe zijn de toezicht en sturing geregeld?
- het tactische niveau: welke afspraken en standaarden zijn ingeregeld, hoe vindt overleg plaats?
- het operationele niveau: hoe zijn de technische voorzieningen ingericht?

Voor een betrouwbaar functioneren van de informatieketens zijn de elementen van deze drie niveaus volgens de NOREA cruciaal en zij verdienen daardoor om door gecertificeerde auditor te worden beoordeeld. Dit betekent derhalve niet alleen beperkte onderzoeken over sturingsvraagstukken maar ook diepgaande uitspraken over de techniek. Immers, “the devil is in the detail”.
De NOREA wil vanuit haar verantwoordelijkheid bijdragen aan een stevig fundament onder de gedigitaliseerde informatieketens binnen de overheid en het bedrijfsleven. De bij haar aangesloten IT-auditors kunnen vanuit hun rol deze beoordeling uitvoeren en adviseren over kwaliteit van techniek, standaarden, afspraken, toezicht en sturing om zodoende een betrouwbare informatieketen te verkrijgen en te behouden. Het doel daarbij is het verbeteren van de werking van informatieketens en het verkleinen van de kans op incidenten.

Het bestuur van de NOREA stelt het op prijs indien u deze Alert in uw Bestuursraad of Directie wilt agenderen om binnen uw organisatie discussie over dit onderwerp op gang te brengen en de in de bijlage genoemde maatregelen te overwegen. De NOREA zet haar diepgaande kennis omtrent betrouwbaarheid van informatiesystemen graag in om u daarbij te ondersteunen. Voor nadere informatie kunt u contact met ons opnemen via het secretariaat (020- 3010380).

Namens het bestuur,

Ir. Ard Niesen RE,
Voorzitter

Bijlage

ONTWIKKELINGEN EN BEDREIGINGEN KETENINFORMATISERING

De IT-auditors die zijn aangesloten bij de NOREA zijn sterk betrokken bij de digitalisering binnen de overheden. Deze betrokkenheid kan zijn vanuit een interne auditdienst zoals de Audit Dienst Rijk, vanuit een auditfirma of doordat zij werkzaam zijn binnen een overheidsorganisatie. Hierdoor ontstaat een breed en onderbouwd beeld van wat zich afspeelt rond de digitalisering. Deze betrokkenheid en kennis is binnen de NOREA gebundeld in de vaktechnische NOREA-werkgroep Ketenauditing. Na een aantal publicaties over dit onderwerp en het geven van lezingen wil de werkgroep haar visie op ketenontwikkeling binnen de Overheid in deze Alert kenbaar maken.

1. VISIE OP KETENONTWIKKELING BINNEN DE OVERHEID

Wanneer de overheid ketens ontwikkelt om uitvoeringsprocessen en koppelvlakken tussen verschillende overheden beter georganiseerd en uitgevoerd te krijgen, gebeurt dit nog vaak vanuit een beperkte optiek van beleidsmakers en wetsjuristen. Een visie op ketenontwikkeling, gericht op samenwerking en samenhang tussen initiatieven, is nog niet ontwikkeld. Door het ontbreken van deze ketenbrede visie ontstaan er tekortkomingen die het optimaal presteren van informatieketens en de ketenpartners belemmeren. Problemen worden vervolgens geïsoleerd beoordeeld en verbeteringen fragmentarisch doorgevoerd. Afstemming tussen beleid, uitvoering, technologie, informatiestromen en netwerken om tot een degelijke visie op ketenontwikkeling te komen wordt steeds urgenter. Professioneel opdrachtgeverschap, creatie van autonomie, vertrouwen, identiteit en imago, het delegeren van besluitvorming en uitbesteding zijn hiervoor belangrijke ingrediënten.

Maatregel 1

Een belangrijke sleutel is het gezamenlijk besturen van de ketens door de betrokken partijen. De spanning die bestaat tussen verticale sturing vanuit de eigenaar en de horizontale verbinding tussen de organisaties verdient het om hierin geadresseerd te worden.

De politieke dynamiek tussen minister, Tweede Kamer en departement bij de wetsbehandeling kan verder stevige invloed hebben op de ontwikkeling van ketens. Een gemeenschappelijke visie op een concrete vertaling van de gewenste wetsuitvoering in werkbare concepten ontbreekt vaak, ook doordat er zelden tijd is voor gedegen uitvoeringsanalyses. De nadruk komt daardoor eenzijdig op de ICT te liggen en te weinig bij organisatorische, samenwerking- en procesaspecten. Hierdoor wordt de besturing zoals hiervoor bedoeld, al te gauw uit het oog verloren. De kloof tussen de overheid als opdrachtgever (een ministerie) en de overheid als feitelijk gebruiker van een ontwikkeld systeem (uitvoeringsorganisaties) lijkt groot. Bij de realisatie van ketensystemen in projecten is te weinig aandacht voor projectoverstijgende aspecten die de eenheid van het toekomstige beleid en uitvoering raken.

Maatregel 2

Voor een goede ketenontwikkeling is het van belang het vertrouwen tussen en de posities van de betrokken organisaties in samenhang te versterken en de besluitvorming naar de samenwerkende partijen te delegeren.

Illustratief voor de problemen is de situatie van de stichting ICTU rond 2010 in haar realisatie van verschillende ketenproducten voor de e-overheid. In het licht van het welslagen van grote ICT-projecten is het problematisch dat ICTU, in haar eigen woorden, een echte projectorganisatie is. Als een projectdoel bereikt is, verdwijnt het bij ICTU uit het zicht, terwijl de overdracht en in gebruikname van de systemen aan de beheerorganisaties en de aansluiting van ketenpartners daarop moeizaam verloopt en kostbaar is. Pas daarna kan de echte afstemming met de dagelijkse praktijk beginnen en breekt de fase van beheer en doorontwikkeling in de informatieketen aan. Dit vraagt ook bij ICTU om een visie op sturing op de samenhang in ketenontwikkeling en -beheer waarbij er aandacht is voor een procesmatige aanpak, het stellen van heldere doelen en het erkennen en afstemmen van de wederzijdse belangen.

2. VERTROUWEN EN GOED BESTUUR

De situatie die de hack op de site van DigiNotar in 2011 opleverde is te omschrijven als een acuut gebrek aan vertrouwen. Waar DigiNotar bedoeld was om vertrouwen te geven in het onderling zakendoen, ontstond in zeer korte tijd een grote verwarring binnen het Rijk, Gemeenten en Uitvoeringsorganisaties. Er was niet gerekend op de snelheid waarmee het vertrouwen in alle sites en koppelingen binnen informatieketens werd opgezegd. Het bijzondere was wellicht dat Microsoft als commerciële provider deze druk hoog opvoerde door haar programma Explorer voor sites met certificaten van DigiNotar af te sluiten. Hierdoor moesten certificaten in een hoog tempo en soms in aantallen van honderden per organisatie worden vervangen. Dat de aandacht en onderzoeken werden gericht op sites die voorzien waren van betrouwbaarheidscertificaten is vanuit het gezichtspunt van goed bestuur begrijpelijk. De meeste andere onderzoeken zijn eveneens gericht op techniek en beheer. Het grote vraagstuk dat vertrouwen in een vernetwerkte digitale overheid is, heeft tot nu toe nauwelijks aandacht getrokken. Wellicht dat de lopende onderzoeken vanuit de Tweede Kamer en de Onderzoeksraad voor de Veiligheid hier licht op kunnen werpen. De kwetsbaarheid die netwerken en informatieketens met zich mee brengen zouden geadresseerd moeten worden als belangrijke onderwerpen binnen goed bestuur. De crisisachtige situatie rondom DigiNotar illustreert het feit dat een fout in een proces van de ene organisatie onmiddellijk doorwerkt in die van een andere organisatie.

Maatregel 3

In een goed georganiseerde samenwerking in informatieketens kan men preventief maatregelen treffen om vertrouwen te borgen. Het voorbereiden op het zo snel mogelijk beperken van de gevolgen in geval van calamiteiten en het schenden van vertrouwen in te dammen hoort daarbij. Zelfbewuste eigenaren en opdrachtgevers die audit en onderzoek gebruiken als sluitstuk van Goed Bestuur bieden daarvoor de verankering.

3. BEHEERSING EN CONTROLE VAN KETENS

In haar rapport in 2012 concludeert de WRR, dat in de dagelijkse digitale praktijk een iOverheid is ontstaan die volop 'draait' op nieuwe informatiestromen die door ICT mogelijk zijn gemaakt. Door een overvloed aan allerlei informatie veranderen het functioneren en het karakter van zowel de samenleving als de overheid. Soms is dit duidelijk aanwijsbaar, maar soms gebeurt het ook op een meer sluipende wijze. De combinatie van nieuwe technologieën, open specificaties, innovatieve architecturen en de beschikbaarheid van overheidsinformatie kunnen voor burgers en bedrijfsleven

een meerwaarde opleveren. Evident is dat deze trends en ontwikkelingen direct invloed uitoefenen op de rol, organisatie en dienstverlening van overheden, maar ook op de relatie tussen overheid, burgers en bedrijfsleven. Twee belangrijke hoofdstromen hebben zich hierin ontwikkeld: de gezamenlijke dossiers, waar meerdere partijen gebruik van maken en ketens, waarin informatie volgtijdelijk wordt verwerkt en gebruikt. Authentieke registers in Nederland worden in beide stromen gebruikt.

Maatregel 4

De overheid die massaal gebruik maakt van informatiestromen en informatienetwerken, zal haar beleid, uitvoering en toezicht daarop moeten aanpassen.

Door het koppelen en uitwisselen van informatie vervagen de traditionele grenzen tussen beleidsterreinen en overheidsorganisaties, ook in relatie tot de private sector. De populariteit van gegevensuitwisseling binnen ketens, gefaciliteerd door unieke registratienummers en authentieke registers, maakt dat informatie eenvoudig over de traditionele organisatiegrenzen heen vloeit. De verantwoordelijkheid voor de kwaliteit van de gegevens is bij wet geregeld. Maar daarin is niet de betrouwbaarheid van de informatieketens geregeld. Dit vraagt om een nieuwe blik op beheersing van en verantwoording over deze informatiestromen, zoals bleek uit een onderzoek van de Algemene Rekenkamer in 2012 naar de keten van Aangifte en Opsporing bij Politie en Justitie. Hoe goed en efficiënt politiekorpsen inmiddels aangiften aan elkaar kunnen doorgeven, zij zijn wel de tel kwijtgeraakt en kunnen soms moeilijk verantwoorden wat er met de aangifte van een burger is gebeurd. Met de toenemende informatiestromen wordt het op orde brengen van de papieren en digitale informatie een steeds grotere uitdaging.

Maatregel 5

Voor het afbreken van oude muren en ingesleten processen is de actieve participatie van bestuurders noodzakelijk.

Zonder bestuurlijke grip en doorzettingsmacht van de verantwoordelijke bestuurders zal de dagelijkse ICT-praktijk gepaard blijven gaan met onoverzichtelijkheid en gebrek aan transparantie en verantwoording. In het organisch groeiproces dat de digitale overheid is, kunnen bestuurders veel kansen aanwenden om de groei in goede banen te leiden. De effecten die digitalisering op het functioneren en de verantwoording van overheden heeft, moeten veel meer in kaart worden gebracht en worden bestudeerd. De NOREA kan en wil daarin een actieve rol blijven spelen, immers de discussie mag niet blijven steken in technologie of in financiële debacles.

Maatregel 6

Het is tijd voor de volgende stap: "level 2" in Keteninformatiseren: het formuleren van doelstellingen en inrichten van structuren.

4. COMPLEXITEIT VAN KETENS EN KOPPELVLAKKEN

Van oudsher ligt binnen de ICT de focus op het ontwikkelen en invoeren van applicaties binnen organisaties. Destijds zijn veel applicaties ontwikkeld om specifieke functies in de uitvoering te ondersteunen. Doordat steeds meer procesgericht wordt gewerkt en doordat functies aan elkaar worden gekoppeld beschikt elke organisatie sinds eind vorige eeuw over een lijst van koppelvlakken die de applicaties onderling verbinden. Koppelvlakken vergen veel aandacht omdat zij cruciaal zijn voor betrouwbare gegevensuitwisseling en -verwerking.

In de laatste tien jaar heeft de trend van procesgericht werken zich na het bedrijfsleven ook binnen de overheid, over organisaties heen voortgezet: "De informatieketen is uitgevonden!". Het beheersen van de koppelvlakken blijkt hier veel moeilijker omdat de verantwoordelijkheid niet meer binnen één organisatie ligt. Hoe ernstig de gevolgen van een tekortkoming in een koppeling kunnen zijn, bleek in de loonaangifteketen, waar een grote hoeveelheid data in het koppelvlak bleef "hangen", zonder dat dit werd gemerkt. De oorzaak van dergelijke gebeurtenissen is gelegen in het feit dat het ketenproces niet als een geheel is ontwikkeld en beheerd. Op dit moment is er nog veelal sprake van het ontwikkelen en beheren van deelsystemen, die dan achteraf aan elkaar geknoopt moeten worden. Dit kan worden voorkomen door binnen ketens de kwaliteit van informatie en informatieverwerking gericht op de uitvoeringsprocessen in samenhang te ontwikkelen en te beheren. Heldere referentiekaders om ketens en koppelvlakken zo robuust uit te voeren dat bij storingen op een voorspelbare manier herstel van de informatie-uitwisseling plaatsvindt, zijn hierbij nodig.

Maatregel 7

Bestuurders van organisaties binnen ketens zullen hiervoor de handen ineen moeten slaan, waar mogelijk met de verantwoordelijke voor de keten. IT-auditors kunnen behulpzaam zijn bij het uitvoeren van risicoanalyses, het onderzoeken en documenteren van de betrouwbaarheid van de keten, en ook bij het ontwikkelen van control frameworks.

5. VOLWASSENHEIDSNIVEAUS IN KETENS

Met de inrichting van ketens om de uitvoeringsprocessen in de publieke sector efficiënter en effectiever te organiseren ontstaan afhankelijkheden tussen de bij een keten betrokken organisaties. Het verschil in volwassenheidsniveau van organisaties leidt gemakkelijk tot een spanning in de keten, indien hiervoor onvoldoende oog is. Door de samenwerking in ketenverband krijgen onderdelen van de keten een kritieke rol in de processen van collega-organisaties, vaak zonder dat zij daarvoor zijn ingericht en voorbereid. Die spanning leidt op een gegeven ogenblik tot een ernstige hinder in de uitvoeringsprocessen van de betreffende organisaties. Treffende voorbeelden van dit fenomeen, waarbij uitvoeringsprocessen stil kwamen te liggen, zijn de beschreven problemen in de Loonaangifteketen en het DigiNotar incident in 2011. Organisaties die een voldoende volwassenheidsniveau hebben beschikken over crisisscenario's waarmee zij in staat zijn om binnen redelijke termijn hun dienstverlening weer op peil te hebben. Bij de crisis rond DigiNotar bleken er rondom beveiligingscertificaten geen scenario's beschikbaar te zijn. Het ontbreekt nog aan een gemeenschappelijke risicoanalyse en scenario's en afspraken om de goede werking van informatieketens te borgen, conform de eisen die de meest kritische uitvoeringsprocessen stellen. Deze afspraken dienen zich in elk geval uit te strekken over het ontwerp van koppelvlakken, de kwaliteit van de gebruikte infrastructuur en de wijze van omgaan met en herstel fouten en uitval.

Maatregel 8

Op ketenniveau zijn afspraken nodig over het versterken van de 'zwakke schakels', waarbij aan ketenpartners eisen moeten en kunnen worden gesteld.

6. TECHNISCHE KWETSBAARHEID OP COMPONENTENNIVEAU

In complexe informatieketens is sprake van een overvloed aan componenten waarover de uitwisseling van gegevens plaatsvindt. In een dergelijk complexe infrastructuur kan sprake zijn van verouderde componenten die weinig tot geen ingebouwde beveiliging hebben. Een recent voorbeeld hiervan is te zien geweest bij de inbraak in het IT-netwerk van KPN in 2012 door een hacker waardoor gegevens van klanten en de dienstverlening in gevaar kwamen. Naar aanleiding van deze hack werd alle klanten geadviseerd hun wachtwoord te wijzigen. Deze hack was prima te voorkomen geweest als systemen beter onderhouden zouden zijn geweest, oude lekken gaven nu echter toegang.

Maatregel 9

IT-audits zijn bedoeld om dit soort kwetsbaarheden bloot te leggen en bestuurders in staat te stellen verbeteringen aan te brengen.

Een ander voorbeeld is de brand bij een knooppunt van Vodafone in 2012. In de regio Rotterdam - Den Haag was mobiel bellen, SMS- en internetverkeer voor klanten van Vodafone (waaronder het grootste deel van de Rijksambtenaren) dagenlang onmogelijk doordat circa 700 zendmasten niet meer werkten. Voor een belangrijk deel van de klanten elders in het land bleek de uitval van een authenticatieserver tot grote problemen te leiden. Uitwijkvoorzieningen bleken niet adequaat te zijn geregeld.

Een weinig robuuste koppeling in de Loonaangifteketen leidde tot verlies van gegevens met grote gevolgen voor bedrijven, Belastingdienst en het UWV. Jaaraangiften over 2006 moesten massaal opnieuw worden gedaan en bij de organisaties leidde dit incident tot veel herstelwerk.

Deze voorbeelden geven aan dat (op het oog kleine) technische omissies en kwetsbaarheden in componenten van een informatieketen tot (grote) politieke en maatschappelijke schade en onrust leidt. Domino-effecten en grootschalige uitval van netwerken door uitval van componenten zullen moeten worden uitgesloten.