NORA 2.0 principe	Tekst NORA 2.0 Principe	NORA 2014-02-10 Afgeleid Principe
5.1.1	Overheidsorganisaties zijn soevereine deelnemers binnen de e-overheid.	3,4
5.1.1.1	De interne besturing van organisaties is gebaseerd op planning en controle met gebruikmaking van adequate prestatie-indicatoren.	31,33
5.1.1.2	Overheidsorganisaties werken systematisch aan kwaliteitsverbetering.	31
5.1.2	De functies van overheidsorganisaties zijn inzichtelijk.	3,4
5.1.3	Overheidsorganisaties werken binnen de e-overheid samen.	3
5.1.4	De architectuur opbouw van overheidsorganisaties is gericht op het verlenen van diensten aan burgers en bedrijven via meerdere kanalen, evenals op onderlinge samenwerking door het koppelen van dienstverleningsprocessen.	2,8,9
5.1.5	Overheidsorganisaties werken samen aan diensten aan burgers en bedrijven op basis van een service-georiënteerde architectuur.	1,2
5.2.1.1	Overheidsorganisaties bieden op transparante wijze nauwkeurig omschreven diensten aan.	5
5.2.1.2	Tot de kwaliteitsindicatoren van een (combinatie)dienst behoren op zijn minst: juistheid, volledigheid doorlooptijd, rechtmatigheid.	5
5.2.1.3	Diensten moeten SMART beschreven worden.	5
5.2.1.4	Per dienst wordt een normbewerkingstijd en een daarvan afgeleide kostprijs vastgesteld	5,28
5.2.1.5	Service- en dienstbeschrijvingen moeten gerelateerd worden aan een semantisch model waarin de betekenis van de service of dienst staat uitgedrukt.	5
5.2.1.6	Diensten van de overheid die via verschillende kanalen worden geleverd moeten hetzelfde resultaat voor de afnemer van de dienst opleveren.	10
5.2.1.7	Diensten kunnen ook in combinatie geleverd worden: combinatiediensten.	20
5.2.1.8	Dienstverlening gaat over organisatiegrenzen heen.	1,2
5.2.1.9	Organisaties in het publieke domein verlenen hun diensten via ten minste de volgende kanalen: Internet, telefoon, post en balie.	7,8
5.2.1.10	Bij de overheid bent u nooit aan het verkeerde adres: “no wrong door”.	21
5.2.1.11	Stimuleren kanaalgebruik met beste kosten/kwaliteit-verhouding.	4
5.2.1.12	Kanalen bieden gelijke diensten en werken gelijkvormig.	11
5.2.1.13	Organisaties in het publieke domein attenderen burgers en bedrijven op voor hen relevante diensten (proactieve dienstverlening).	21,22,23
5.2.1.14	Burgers krijgen door middel van het burgerservicenummer een digitale, unieke identiteit. Dit BSN dient maximaal door overheidsorganisaties te worden toegepast.	36
5.2.1.15	Bedrijven en instellingen krijgen door middel van het bedrijven- en instellingennummer een digitale, unieke identiteit.	36
5.2.1.16	De klant wordt op een persoonlijke manier benaderd.	19
5.2.1.17	Diensten die centraal worden aangeboden vergen een overheidsbreed coördinatiemechanisme.	5,27
5.2.1.18	Dienstverleningskanalen zijn ingericht vanuit het perspectief van de klant.	18
5.2.2.1	Diensten en services kunnen worden samengesteld door middel van andere services.	1,6,21
5.2.2.2	Het centraal aanbieden van services wordt gecoördineerd door een overheidsbreed coördinatiemechanisme.	6,27
5.2.2.3	Overheidsorganisaties maken afspraken over het verlenen van services.	26,27
5.2.2.4	De eisen die worden gesteld aan diensten, zoals kwaliteit, telbaarheid en kostprijs, worden ook gesteld aan services.	28
5.3.1	Services triggeren elkaar en kunnen hierdoor processen verbinden.	23
5.3.2	De procesarchitectuur is bij voorkeur gebaseerd op de decompositie ketenproces-bedrijfsproces, werkproces-processtap of handeling.	vervallen
5.3.3	De besturing van ketenprocessen dient door de betrokken organisaties eenduidig geregeld te worden.	5

NORA 2.0 principe	Tekst NORA 2.0 Principe	NORA 2014-02-10 Afgeleid Principe
5.3.4	Klanten hebben de mogelijkheid zich op de hoogte te stellen van de stand van zaken van de uitvoering van de dienstverlening.	24
5.3.5	Een administratief proces is opgesplitst in een invoer-, verwerking- en uitvoerproces.	vervallen
5.3.6	Informatie wordt éénmalig uitgevraagd.	11
5.3.7	Processen dienen te worden beschreven op basis van algemeen geaccepteerde en open standaarden.	7
5.3.8	Processen die geautomatiseerd worden uitgevoerd, dienen beschreven te worden m.b.v. een algemeen erkende (open) standaard.	5,8
5.3.9	Processen worden zodanig ontworpen dat procesgegevens systematisch kunnen worden vastgelegd.	vervallen
5.3.10	Maak bij het kiezen van overdrachtsmomenten in processen een expliciete afweging tussen doorlooptijd en kwaliteit van het proces.	4,5
5.3.11	Procesbeschrijvingen moeten gerelateerd worden aan een semantisch model waarin de betekenis van de betrokken activiteiten staat.	5
5.3.12	Ketenprocessen kunnen ontworpen worden door middel van het interactieperspectief.	vervallen
6.1.1.1	De uitvoering van processen gebeurt door een maximale inzet van ICT.	1
6.1.1.2	Applicaties voeren services van slechts één functioneel domein uit.	1
6.1.1.3	Organisaties en applicaties die in verschillende functionele domeinen werkzaam zijn, werken met elkaar samen op basis van services.	1
6.1.1.4	De applicatiearchitectuur van een overheidsorganisatie bestaat uit meerdere lagen en typische functionele domeinen.	vervallen
6.1.1.5	De uitvoering van handmatige taken in werkprocessen en processtappen wordt bij voorkeur ondersteund met een workflowmanagement.	vervallen
6.1.1.6	De besturing van bedrijfsprocessen geschiedt door de inzet van businessprocesmanagementsystemen.	vervallen
6.1.1.7	Voor het ondersteunen van de controlefunctie van een organisatie kan gebruik gemaakt worden van een managementinformatiesysteem.	vervallen
6.1.1.8	Applicaties maken gebruik van de standaard faciliteiten van hun omgeving.	6
6.1.1.9	Ontwikkelstraten maken gebruik van internationale open standaarden t.a.v. frameworks voor toolsets en methoden en technieken voor software-ontwikkeling.	8
6.1.2.1	Dienstverleningskanalen sluiten waar mogelijk aan op de generieke bouwstenen van de e-overheid.	6
6.1.2.2	Websites van overheidsorganisaties zijn ontwikkeld en ingericht conform de ‘overheidswebrichtlijnen’.	6
6.1.2.3	Wanneer een dienst via meerdere kanalen wordt geleverd, moet het mogelijk zijn bij elk interactiemoment tussen overheid en dienst het optimale kanaal te kiezen.	11
6.1.2.4	Indien gegevens aan klanten gevraagd worden, mag uitvraag ervan over meerdere processtappen worden verdeeld.	11
6.1.2.5	Frontoffice-applicaties kennen een beperkte controletaak op de kwaliteit van de gegevens.	vervallen
6.1.2.6	Inkomende en uitgaande formele communicatie met klanten wordt gearchiveerd.	29
6.1.3.1	Complexe services mogen gebruikmaken van eenvoudige services.	1,3,6
6.1.3.2	Services zorgen voor een losse koppeling tussen gebruiker en leverancier.	1
6.1.3.3	Bij services die deel uitmaken van een bedrijf- of werkproceskoppeling van transactionele aard is een transactieprotocol (met compenserende acties) aanwezig.	35
6.1.3.4	Service-informatie is landelijk beschikbaar.	5,6
6.2.1.1	Gegevens, documenten en berichten worden voorzien van metagegevens ten behoeve van ontsluiting van de informatie.	16
6.2.1.2	De afnemer van informatie mag niets merken van wijzigingen in het beheer van de informatie.	34
6.2.1.3	Beleid en regelgeving moeten in onderlinge samenhang via Internet ontsloten kunnen worden. Hiervoor worden de richtlijnen gevolgd.	vervallen

NORA 2.0 principe	Tekst NORA 2.0 Principe	NORA 2014-02-10 Afgeleid Principe
6.2.3.1	Binnen de e-overheid worden metagegevens geregistreerd op het moment dat brongegevens worden ontvangen of zaakgegevens wijzigen. Bij voorkeur geschiedt dit automatisch.	17,36
6.2.3.2	Overheidsorganisaties houden bij de registratie van gegevens rekening met digitale duurzaamheid.	29
6.2.3.3	Gegevens, berichten en documenten worden voorzien van metagegevens ten behoeve van beheer.	16,17
6.2.3.4	Elk gegeven kent een eigenaar en een beheerder.	13,27
6.2.3.5	De eigenaar van een gegeven is verantwoordelijk voor de kwaliteit (actualiteit, betrouwbaarheid) van een gegeven.	13,27,35
6.2.3.6	Gegevensverzamelingen die eigendom zijn van een overheidsorganisatie worden – met inachtneming van nadere wettelijke regels - ter beschikking gesteld aan de gehele overheid.	1,2,13
6.2.3.7	Van geleverde gegevens is de kwaliteit bekend.	30,33,35
6.2.3.8	Content wordt zoveel mogelijk kanaalonafhankelijk opgeslagen en aangeboden.	11
6.2.4.1	Gegevens- en procesinhoudelijke communicatiestandaarden moeten een semantisch model bevatten of verwijzen naar een semantisch model.	4
6.2.4.2	Semantische modellen zijn technologieneutraal.	1,5,17
6.2.4.3	Het bepalen van de passende omvang van een semantisch model is maatwerk.	vervallen
6.2.4.4	Waar haalbaar onderscheidt een semantisch model expliciet objecten en gebeurtenissen.	vervallen
6.2.4.5	De definitie en taxonomie van gegevens die zijn opgenomen in nationale basisregistraties zijn leidend.	6,13
6.2.4.6	Binnen de e-overheid worden gegevens die door meerdere organisaties gebruikt (kunnen) worden zoveel mogelijk volgens (inter)nationale standaarden gedefinieerd.	6,13
6.2.4.7	De vervuiler vertaalt.	28
6.2.6.1	Overheidsorganisaties maken gebruik van de (Nederlandse) basisregistraties.	12
6.2.6.2	Bij elk gegeven dat wordt gebruikt door meerdere overheidsorganisaties moet duidelijk zijn welke organisatie leidend is. Deze organisatie bepaalt of een wijziging doorgevoerd mag worden.	12,13,14,27
6.2.6.3	Een verandering in de administratieve werkelijkheid wordt ter attentie gebracht van alle partijen die daar belang bij hebben.	27
6.2.6.4	Verschillen tussen gegevens in basisregistraties en andere bronnen, worden in geval van gerede twijfel, via een vaste procedure gemeld aan de beheerder van de betreffende basisregistratie.	13
6.2.6.5	Objecten worden op een systematische wijze beschreven.	17
6.3.1	Het berichtenverkeer binnen de e-overheid wordt vooralsnog gebaseerd op standaarden conform ofwel de ebXML-familie ofwel de Webservice familie.	7
6.3.2	Een bericht bevat een header en pay-load gedeelte.	vervallen
6.3.3	Versiebeheer van berichtenstandaarden wordt ondersteund.	35
6.4.2	Voor berichtentransport worden naast elkaar meerdere protocollen toegepast, waaronder HTTP en FTP. Voor transportroutering wordt DNS gebruikt.	vervallen
6.4.3	Sectorale en de Overheids servicebussen kennen een hoge betrouwbaarheid en zijn 7*24h beschikbaar.	28,35
6.4.4	Doorlooptijd van berichtenverkeer is onderwerp van expliciete afspraak tussen servicebussen en hun gebruikers.	28
6.4.5	Vorige versies van communicatieprotocollen binnen de e-overheid worden gedurende twaalf maanden nog ondersteund.	28,35
6.4.6	De logische koppeling van organisaties aan sectorale bussen geschiedt door businessprocesmanagementoplossingen.	vervallen
6.5.1	Servicebussen gebruiken dezelfde standaards voor berichtenverkeer als de OSB.	6

NORA 2.0 principe	Tekst NORA 2.0 Principe	NORA 2014-02-10 Afgeleid Principe
6.5.2	Koppelingen tussen verschillende sectorale servicebussen lopen altijd via de OSB.	vervallen
6.5.3	Gebruik bij het kiezen van de juiste servicebus omvang en diversiteit als leidraad.	vervallen
7.1.1	Met inachtneming van het belang van beschikbaarheid, interoperabiliteit en beveiliging, zijn overheidsorganisaties relatief vrij in het kiezen van technische componenten.	vervallen
7.1.2	Organisaties die 7*24 dienstverlening aanbieden, zorgen ook voor een bijpassende hoge technische beschikbaarheid van de onderliggende machines en platformen.	35
7.2.1	Gestructureerde gegevensopslag heeft de voorkeur ten opzichte van 'half gestructureerde gegevensopslag'.	vervallen
7.2.1.1	De gegevensstructuur van databases is gegevengericht opgezet.	vervallen
7.2.1.2	Vanuit een gegevensverzameling worden gegevensservices verleend.	vervallen
7.2.1.3	Databasegegevens zijn herleidbaar tot de bron.	13
7.2.2	Gegevensverzamelingen worden op een standaard manier beschreven.	8
7.2.2.1	Documenten die gebruikt worden door meerdere overheidsorganisaties, of door burgers en bedrijven kunnen worden geraadpleegd, worden elektronisch beschikbaar gesteld.	1,13
7.2.3	De Basisregistraties zijn leidend.	12
7.3.1	Communicatie tussen overheidsorganisaties verloopt via besloten, separate netwerken of door middel van een virtual private network-verbinding via netwerken van particuliere bedrijven.	38
7.3.2	Communicatie e-overheid en burgers/bedrijven via een beveiligde Internetverbinding of VPN.	Vervallen
7.3.3	Het interne netwerk van overheidsorganisaties is via één redundant en veilig uitgevoerde koppeling aangesloten op het publieke netwerk.	38,39
9.3.1	Informatiebeveiliging is een integraal aspect van de bedrijfsvoering (corporate governance)	32,34
9.3.2	De leiding van een organisatie is verantwoordelijk voor een toereikende organisatie van informatiebeveiliging.	32
9.3.3	Security-incidenten worden gesignaleerd, vastgelegd en gerapporteerd. Beveiligingsrelevante afwijkingen bij de uitvoering van processen worden aangemerkt als security-incidenten.	39
9.3.4	Samenwerkende organisaties organiseren de vastlegging van relevante gebeurtenissen (event logging, audit logging) met een organisatieoverschrijdend karakter op een inhoudelijk samenhangende wijze	30,33
9.4.1	Organisaties waarborgen de persoonlijke levenssfeer (privacy) van natuurlijke personen door te voldoen aan de eisen uit de WBP.	Vervallen
9.4.2	Overheidsorganisaties betrachten maximale transparantie voor de betrokkenen wat betreft de op hen betrekking hebbende verwerking van persoonsgegevens en verstrekkingen aan derden van die persoonsgegevens, d.m.v. elektronische inzage.	25
9.4.3	In de keten samenwerkende overheidsorganisaties toetsen de toereikendheid van de waarborgen voor de persoonlijke levenssfeer (privacy) van natuurlijke personen.	Vervallen
9.4.4	Overheidsorganisaties operationaliseren de wettelijke eisen aangaande privacy via een managementcyclus van beleid tot en met controle.	31,32,33
9.4.5	Overheidsorganisaties streven naar zelfregulering op het gebied van bescherming persoonsgegevens.	Vervallen
9.4.6	Bij controle op werknemers wordt het privacybelang van de werknemers door de werkgever in acht genomen.	Vervallen
9.4.7	Privacy wordt zoveel mogelijk in het ontwerp van geautomatiseerde systemen geborgd door middel van Privacy Enhancing Technologies.	6,8
9.4.8	Met behulp van encryptie worden bijzonder gevoelige gegevens onleesbaar gemaakt voor ongeautoriseerde kennisname.	33

NORA 2.0 principe	Tekst NORA 2.0 Principe	NORA 2014-02-10 Afgeleid Principe
9.4.9	De door overheidsorganisaties gebruikte ICT-oplossingen zorgen voor een transparante, controleerbare en beheersbare verwerking van persoonsgegevens.	26,20
9.5.1	Organisaties richten een proces in voor de waarborging van de continuïteit van de diensten en services die via hun bedrijfsprocessen worden geleverd.	35
9.6.1	Convergentie van informatiebeveiliging, privacy en continuïteit van de bedrijfsvoering tussen (in ketens of netwerken) samenwerkende organisaties moet het gevaar van “de zwakste schakel” voorkomen.	6,29,35
9.6.2	Samenwerkende organisaties leggen verantwoording af waarin zij de relatie leggen tussen de door hen getroffen maatregelen en de gemaakte keten-/netwerkafspraken.	27,34
9.6.3	Toezicht wordt uitgeoefend met behulp van audits door een onafhankelijke deskundige. De relevante auditresultaten worden beschikbaar gesteld aan de partners in de samenwerking.	34
9.6.4	Op basis van monitoring geeft elke ketenorganisatie zekerheid over de naleving van de ketenafspraken.	28,31,34
9.7.1	Gebruik elektronische handtekeningen bij hoge eisen aan de onweerlegbaarheid van een bericht of transactie. Bovendien worden de documenten of berichten gearchiveerd.	34
9.7.2	Minimaal bij transacties die een verplichting vormen voor een burger of bedrijf/instelling, zal de e-overheidsorganisatie kwijting geven van het afgerond hebben van een transactie/wezenlijke processtap.	25
9.7.3	E-overheidsorganisaties beveiligen de toegang tot hun diensten door middel van generieke authenticatiediensten op basis van DigiD en/of PKI-overheid.	6,7,8,37
9.7.4	E-overheidsorganisaties faciliteren vertegenwoordigingsrelaties in hun elektronische dienstverlening.	20,37
9.7.5	Elektronische diensten worden verleend op basis van een bekende identiteit, waar het gaat om persoonlijke gegevens en transacties.	20,37
9.7.6	Elke overheidsorganisatie kan de handelingen van haar medewerkers (al dan niet in het kader van een aan burger of bedrijf te leveren dienst) intern tot op de persoon herleiden.	30,37,39
9.8.1	Om een service en de onderliggende informatie aantoonbaar goed te beveiligen en in de tijd ook beveiligd te houden, moet elke organisatie een beveiligingscyclus voor de service inrichten.	31,33
9.8.2	De beschikbaarheid van de service is door de eigenaar gedefinieerd en geborgd.	5,28,35
9.8.3	Ketenorganisaties specificeren maatregelen op het gebied van informatiebeveiliging, privacy en continuïteit van de bedrijfsvoering voor specifieke diensten en services, op basis van de met die diensten en services samenhangende risico's.	5,33
9.8.4	De service voldoet aan wet- en regelgeving en contractuele verplichtingen.	28,35
9.8.5	Door middel van (publieke) voorlichting worden klanten van de diensten bewust gemaakt van de risico's en de noodzaak van beveiliging.	vervallen
9.8.6	Let op de beveiliging, privacybescherming en continuïteit van de bedrijfsvoering bij ingekochte diensten.	35,37