Bijlage IV

Een betrouwbare internetstemvoorziening en de onderbouwing daarvan voor het publiek

1. Achtergrond en aanleiding

Vertrouwen van burgers in het verkiezingproces is een grondwettelijk fundament van een democratische rechtstaat. Daartoe dient het verkiezingsproces aan bepaalde waarborgen van betrouwbaarheid te voldoen. De Adviescommissie inrichting verkiezingsproces [1.] onderscheidt de volgende acht waarborgen: Transparantie, Controleerbaarheid, Integriteit, Kiesgerechtigdheid, Stemvrijheid, Stemgeheim, Uniciteit

Wij hanteren de volgende terminologie. De *internetstemvoorziening* is opgebouwd uit een *stem-beheerorganisatie* en een (technisch) *internetstemsysteem*. Het internetstemsysteem bestaat uit de applicatieve programmatuur die wordt geïmplementeerd en beheerd door de stem-beheersorganisatie (ICT technisch, facilitair, personeel etc.). Dat betekent dat het vertrouwen van de burger in internetstemmen zowel verband houdt met het geven van vertrouwen in een ICT product (het internetstemsysteem) als in een beheersorganisatie (het beheer van het internetstemsysteem en gerelateerde processen). De internetstemvoorziening (en daarmee de stem-beheerorganisatie en het internetstemsysteem) zullen worden ontwikkeld door, of onder regie van de verkiezingsorganisatie voor kiezers buiten Nederland.

De situatie dat een partij A (de burger in het geval van verkiezingen) moet vertrouwen in een dienst die wordt uitgevoerd door een andere partij B (de overheid/ministerie van binnenlandse zaken in het geval van verkiezingen) komt vaker voor. Partij B kan bijvoorbeeld een bank zijn die een internet bankieren dienst levert en partij A kan een klant van de bank zijn die zeker wil zijn dat zijn spaargoed veilig is. Partij A kan ook een bedrijf zijn dat zijn administratieve processen inclusief ICT heeft uitbesteed bij partij B en zeker wil zijn dat dit zorgvuldig gebeurt.

De gebruikelijke basis voor het geven van vertrouwen in een product of een beheersorganisatie bestaat eruit zorg te dragen dat:
a) de betrouwbaarheid hiervan voldoende is geborgd, en
b) dat voldoende informatie wordt verstrekt aan afnemende partijen om dit te aan te tonen.

Voor het geven van dit vertrouwen kan gebruik worden gemaakt van bestaande standaarden die wij onderstaand zullen bespreken.

Dit hoofdstuk is als volgt opgebouwd:
- Sectie 2 bevat de centrale conclusie van dit hoofdstuk en doet een voorstel voor het geven van publiek vertrouwen in de internetstemvoorziening en de twee belangrijke componenten daarin, dat wil zeggen de stem-beheerorganisatie en het (technische) internetstemsysteem;
- Sectie 3 gaat in op de borging van de betrouwbaarheid van de internetstemvoorziening;
- Sectie 4 gaat in op de wijze waarop de geborgde betrouwbaarheid van de internetstemvoorziening publiekelijk kan worden onderbouwd;
- Sectie 5 bevat een overzicht van de gebruikte referenties;
- Sectie 6 gaat over de ISO 27001 standaard.

2. Conclusie

De internetstemvoorziening is opgebouwd uit twee componenten: een stem-beheerorganisatie en een (technisch) internetstemsysteem. Voor het geven van vertrouwen aan de burger in de betrouwbaarheid van de internetstemvoorziening dient enerzijds de betrouwbaarheid hiervan geborgd zijn en dient er anderzijds ook voldoende informatie te worden verstrekt aan het publiek om dit te onderbouwen. Voorstellen voor de realisatie van elke van deze twee punten zijn onderstaand beschreven.

Voor de borging van de betrouwbaarheid van de twee componenten van de internetstemvoorziening stellen wij het volgende voor:

- Voor de stem-beheersorganisatie stellen wij adoptie van de ISO 27001 standaard ([2.]) voor. Dit is de leidende standaard voor management van informatiebeveiliging en is recent ook geadopteerd in het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007).
- Om de betrouwbaarheid van het internetstemsysteem te kunnen borgen dient de betrouwbaarheid van de gehele softwareontwikkelcyclus daarvan (functionele specificatie, ontwikkeling, testen, acceptatie, productie, onderhoud) hiervan geborgd te zijn. Dit omvat meer dan alleen borgen dat het systeem geen puur technische beveiligingszwakheden heeft. Voor de borging van de betrouwbaarheid van de gehele softwareontwikkelcyclus komt in de literatuur een tweetal standaarden naar voren. De tamelijk pragmatische standaard van het Amerikaanse NIST (SP 800-64, zie [9.]) en de meer formalistische ISO 15408 standaard ('*Common Criteria*', zie [10.]). Laatstgenoemde standaard kan in theorie een hogere zekerheid realiseren maar levert door zijn diepgang ook risico's op rond kosten en doorlooptijd. Binnen de beperktheid van het BVIS programma zijn wij niet in staat om een goede keuze te maken van een standaard. Wij stellen daarom voor dat de ontwikkeling en het onderhoud van het internetstemsyteem minimaal onderhevig moet zijn aan de NIST standaard SP 800-64 en dat in het kader van de verdere ontwikkeling van de internetstemvoorziening moet worden onderzocht of andere standaarden, waaronder met name de *Common Criteria,* moeten worden opgelegd.

Voor de onderbouwing van deze borging aan het publiek stellen wij het volgende voor:

- Als basis wordt de stem-beheersorganisatie formeel gecertificeerd tegen de ISO 27001 standaard waarbij het ISO 27001 certificaat gepubliceerd wordt. Hiervoor is in Nederland reeds een formele certificering structuur beschikbaar die ontwikkeld is door ECP.NL en waarop de Raad voor Accreditatie toeziet. Het structureel uitvoeren van een risico analyses speelt een prominente rol binnen ISO 27001 en hierbij zullen de beveiligingskritische onderdelen van het internetstemproces aan het licht komen, zoals: de installatie van het internetstemsysteem en de onafhankelijke waarneming van het stemproces. Specifieke audit aandacht – vastgelegd in een auditplan en uitmondend in aanvullende audit verklaringen – moet hiernaar uitgaan. Behalve het ISO 27001 certificaat kan ook worden overwogen meer onderbouwende informatie te publiceren rond de beveiliging van de stem-beheersorganisatie zoals de centrale risico-analyse en het *Statement of Applicability* dat de basis vormt voor de ISO 27001 certificering.
- Een onafhankelijke auditor (aangewezen door de Kiesraad) voert een onderzoek uit naar de toepassing van de geadopteerde standaarden rond informatiebeveiliging binnen de softwareontwikkelcyclus van het internetstemsysteem en geeft hier een publieke mededeling over af. In het licht van het bovenstaande omvatten deze standaarden dus minimaal de NIST standaard SP 800-64 [9.]. Behalve deze mededeling kan ook overwogen worden meer onderbouwende informatie te publiceren rond de beveiliging van het internetstemsysteem, zoals risico-analyses, lijsten met getroffen maatregelen en delen van de broncode.

3. Borging betrouwbaarheid internetstemvoorziening

3.1 Borging betrouwbaarheid algemeen

Hoewel ICT producten en beheer daarvan verschillend van aard zijn, is het managementsysteem om de kwaliteit daarvan te borgen in hoofdlijn hetzelfde:

1. De betrouwbaarheidseisen waaraan het product / beheer moeten voldoen, worden in overleg met de afnemende partijen bepaald en vastgelegd. Deze betrouwbaarheidseisen moeten vervolgens middels een risico analyse worden vertaald naar (beveiliging) maatregelen in het product / beheer. ('Plan')
2. De maatregelen moeten worden geïmplementeerd in het product / beheer. ('Do')
3. Er moet periodiek worden toegezien dat:
   - De betrouwbaarheidseisen en de daarop gebaseerde risico analyse nog actueel zijn.
   - De maatregelen adequaat zijn toegepast en dat zij effectief zijn en blijven. ('Check')
4. Als de betrouwbaarheidseisen en de daarop gebaseerde risico analyse niet meer actueel zijn of als de effectiviteit van maatregelen om een of andere reden verminderd is, bijvoorbeeld als gevolg van een veranderende bedreigingen, dan moet dat het managementsysteem tijdig voorzien in veranderingen in stappen 1 of 2. ('Act')

Essentieel is dat het management van de verkiezingsorganisatie nauw betrokken is bij de uitvoer van deze stappen en dat dit toeziet dat deze adequaat worden gevolgd. Als basis voor de betrouwbaarheidseisen in de Plan fase kan gebruik gemaakt worden van de acht eisen geformuleerd door de Adviescommissie inrichting verkiezingsproces [1.], te weten: Transparantie, Controleerbaarheid, Integriteit, Kiesgerechtigdheid, Stemvrijheid, Stemgeheim, Uniciteit.

3.2 Borging betrouwbaarheid internetstembeheersorganisatie

Er bestaan verschillende (de facto) standaarden om de borging rond de betrouwbaarheid van een beheersorganisatie vorm te geven. De belangrijkste zijn:

- ISO 27001 'Information Security Management Systems Requirements'

De ISO 27001 standaard [2.] beschrijft een management systeem voor informatiebeveiliging dat vergelijkbaar is met het management systeem voor kwaliteit beschreven in ISO 9001. Dit systeem dat Information Security Management System (ISMS) heet, heeft als doel dat op systematische en adequate wijze beveiligingsmaatregelen ('controls') worden gekozen en toegepast. De ISO 27001 standaard beschrijft daarbij per bovenstaand onderscheiden onderdeel (Plan, Do, Check en Act) specifieke eisen voor.

Het ISMS dient daarom een beargumenteerde keuze te maken uit beveiligingsmaatregelen die staan beschreven in een andere ISO standaard (ISO 27002) getiteld 'Code of practice for information security management' [3.]. Deze keuze dient gedocumenteerd te worden in een zogenaamd 'Statement of Applicability'. De ISO 27002 kan gezien kan worden als een verzamelplaats van allerhande *good practice* beveiligingsmaatregelen. De ISO 27002 omvat 11 hoofdstukken met beschrijvingen van beveiligingsmaatregelen op de verschillende terreinen zoals rond personele beveiliging ('functiescheiding') en cryptografische beveiliging. Voor meer achtergrond informatie rond deze standaard verwijzen wij naar de bijlage.

- CobiT

Control Objectives for Information and related Technology (CobiT, zie [6.]) is een raamwerk voor het gestructureerd inrichten en beoordelen van een IT-beheeromgeving. CobiT omvat meer dan alleen betrouwbaarheid en omvat ook richtlijnen rond de effectiviteit van IT gebruik. CobiT is vanaf 1992 ontwikkeld door het Information Systems

Audit and Control Association (ISACA) en het IT Governance Institute (ITGI). CobiT is mede gebaseerd op ISO standaarden 27001 en 27002.

- ITIL

Information Technology Infrastructure Library (ITIL, zie [7.]) is ontwikkeld als een referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie. ITIL is geen methode of model, maar een set van *good practices*. ITIL kent ook een module voor informatiebeveiliging die gebaseerd is op de eerder genoemde ISO standaarden 27001 en 27002.

Om de volgende redenen stellen wij voor dat de ISO standaard 27001 wordt gehanteerd voor de borging van de betrouwbaarheid van de stem-beheersorganisatie:

- De reikwijdte van de ISO 27001 standaard beperkt zich tot informatiebeveiliging en sluit daarom beter aan op de behoefte dan CobiT of ITIL.
- De ISO 27001 standaard is de onomstreden, leidende standaard voor informatiebeveiliging. Hetgeen blijkt uit het feit dat bredere standaarden zoals CobiT en ITIL zich voor informatiebeveiliging op ISO 27001 baseren. De standaard wordt ook wereldwijd door organisaties toegepast die leidend zijn op het terrein van informatiebeveilging zoals ondermeer Shell, waarbij nog wordt opgemerkt dat deze organisaties ook de initiators waren voor de totstandkoming van de voorloper van deze standaard, de British Standard 7799.
- De standaard is recent overgenomen in het nieuwe Voorschrift Informatiebeveiliging Rijksdienst 2007 dat van toepassing is op de 'Rijksdienst waartoe gerekend worden de Ministeries met de daaronder ressorterende diensten, bedrijven en instellingen.'
- Er bestaat een standaard raamwerk ('certificering') waarmee organisaties kunnen aantonen aan de ISO 27001 standaard te voldoen. Zie ook Sectie 4.1.

3.3 Borging betrouwbaarheid internetstemsysteem

Om de betrouwbaarheid van het internetstemsysteem te kunnen borgen dient de betrouwbaarheid van de gehele softwareontwikkelcyclus daarvan (functionele specificatie, ontwikkeling, (acceptatie) testen, productie, onderhoud) hiervan geborgd te zijn. Dit omvat bijvoorbeeld dat bij de initiatie van het ontwikkeltraject op basis van een risico-analyse de beveiligingseisen zijn vastgelegd alsmede de opzet van de beveiligingsmaatregelen. Hierbij worden niet alleen 'technische' risico's (zoals bijvoorbeeld *SQL injection* en *bufferoverflow* aanvallen) meegenomen, maar nadrukkelijk ook risico's die samenhangen met het bedrijfsproces dat gebruik maakt van het systeem. In het geval van het internetstemsysteem betekent dat dat de acht eisen geformuleerd door de Adviescommissie inrichting verkiezingsproces [1.] vertaald moeten worden in beveiligingsmaatregelen. In de gehele softwareontwikkelcyclus zijn de opgestelde eisen de rode draad en bij bijvoorbeeld testen wordt niet alleen de functionaliteit getest maar ook wordt getest of voldaan is aan de beveiligingseisen. Ook bij veranderingen in (de broncode) van het systeem moeten deze eisen weer getoetst worden. Veranderingen mogen overigens slechts volgens een stringent *change management* proces plaatsvinden. Resumerend stellen we dat de borging rond de betrouwbaarheid van ICT-producten veel meer omvat dan alleen het zorg dragen dat het systeem geen puur technische beveiligingszwakheden heeft.

Voor deze borging van de betrouwbaarheid van de gehele softwareontwikkelcyclus bestaan verschillende (de facto) standaarden. Wij noemen:

- ISO standaard 12207 "Information technology - Software life cycle processes" Deze standaard [8.] beschrijft de verschillende stadia binnen de softwareontwikkelcyclus (Aquisition, Supply, Development, Operation, Maintenance) en onderscheidt daarin de benodigde processen en activiteiten. De standaard concentreert zich op software kwaliteit maar informatiebeveiliging van de software komt ook zijdelings aan bod.
- NIST Special Standard 800-64 'Security Considerations in the Information System Development Life Cycle'

Deze standaard van het Amerikaanse National Institute of Standards and Technology onderscheidt ook verschillende stadia binnen de softwareontwikkelcyclus maar concentreert zich daarbij op de informatiebeveiliging van de software. Zonder dat zo te noemen wordt daarbij een Plan-Do-Check-Act cyclus onderscheiden waarbij in de Plan fase – *voor* de ontwikkeling of aankoop van het systeem – de functionele beveiligingseisen moeten worden ontwikkeld op basis van een risico analyse en vervolgens vastgelegd; dit omvat ook de beveiligingseisen die worden gesteld in de toekomstige productieomgeving. De beveiligingseisen worden vervolgens bij het verdere ontwikkeltraject (ontwikkeling, testen, in productie name, onderhoud) als randvoorwaarden gehanteerd. De NIST standaard biedt veel praktische handreikingen.

- ISO standaard 15408 '*Common Criteria*'
  Ook deze standaard [10.] concentreert zich op informatiebeveiliging in de softwareontwikkelcyclus. De standaard bestaat uit drie delen: Introduction and general model, Security functional requirements en Security assurance requirements. In beginsel zijn de NIST standaard SP 800-64 en de *Common Criteria* compatibel. Laatst genoemde voorziet echter in een veel formeler en daarmee in beginsel kwalitatief beter traject voor de realisatie van betrouwbare software. Zo zijn er strikte specificaties om beveiligingeisen te beschrijven (resulterend in zogenaamde Protection Profiles en Security Targets). De *Common Criteria* stellen ook strikte eisen aan het evalueren van de beveiliging van software. Dit dient te gebeuren door speciaal geaccrediteerde laboratoria (in Nederland is dat de organisatie Brightsight een spin-off van TNO) en onder strikte procedures. De *Common Criteria* onderscheidt daarbij ook verschillende maten zekerheid (de zogenaamde EAL levels) die testen kunnen geven.

Idealiter zou men wensen dat alle drie de bovenstaande standaarden worden gehanteerd bij de ontwikkeling van het internetstemsysteem. Dit wordt echter naar alle waarschijnlijkheid te complex. De verkiezingsorganisatie zou ook op basis van deze en andere standaarden een eigen normenkader kunnen opstellen. Dit levert echter een onderhoudsprobleem op (wat te doen met het eigen normenkader als de drie standaarden veranderen?). Een ernstiger bezwaar is dat de verkiezingsorganisatie een mogelijk *conflict of interest* kan worden verweten: de verkiezingsorganisatie wil namelijk niet alleen een veilig internetstemsysteem maar heeft ook deadlines te halen en kan daarmee in de verleiding komen het normenkader beperkt te houden. Om deze redenen stellen wij voor om tot een keuze te komen van één beveiligingsstandaard van toepassing op de softwareontwikkelcyclus van het internetstemsysteem.

De NIST standaard is pragmatischer dan de *Common Criteria* standaard en daarmee waarschijnlijk ook minder complex (en kostbaar) in toepassing. De *Common Criteria* standaard geeft in principe echter weer meer zekerheid. Binnen de beperktheid van het BVIS programma zijn wij niet in staat om een goede keuze te maken voor een standaard.

Wij stellen daarom voor dat de ontwikkeling en het onderhoud van het internetstemsyteem minimaal onderhevig moet zijn aan de NIST standaard SP 800-64 en dat in het kader van de verdere ontwikkeling van de internetstemvoorziening moet worden onderzocht of andere standaarden waaronder met name de *Common Criteria* moeten worden opgelegd.

4. Publieke onderbouwing betrouwbaarheid internetstemvoorziening

Zoals wij eerder hebben aangegeven bestaat de internetstemvoorziening uit een stem-beheerorganisatie en een (technisch) internetstemsysteem. Om de betrouwbaarheid van de dienst te kunnen onderbouwen aan het publiek moet zowel de betrouwbaarheid van de stem-beheerorganisatie als die van het (technische) internetstemsysteem publiekelijk onderbouwd kunnen worden.

4.1 Publieke onderbouwing betrouwbaarheid stem-beheersorganisatie

In Sectie 3.2 hebben wij voorgesteld om de betrouwbaarheid van de stem-beheerorganisatie te borgen middels adoptie van de ISO 27001 standaard door de stem-beheerorganisatie. Rond de ISO 27001 standaard is wereldwijd een formele certificering structuur beschikbaar waarbinnen organisaties de mogelijkheid hebben om gecertificeerd te worden tegen de ISO 27001. Hierbij fungeert het zogenaamde Statement of Applicability opgesteld door de organisatie als basis.

In Nederland is deze structuur opgezet door ECP.NL middels een zogenaamd ISO 27001 certificatieschema ('spelregels', zie [11.]) en waarbij de Raad voor Accreditatie (RvA) toeziet op de kwaliteite van auditor organisaties (Certification Bodies). Overigens zal naar verwachting het ECP.NL ISO 27001 certificatieschema op termijn vervangen worden door ISO 27006, zie [5.]. In Nederland zijn een kleine twintig organisaties ISO 27001 gecertificeerd (zie www.ecp.nl). Wereldwijd zijn dit er ruim 4000 (zie http://www.iso27001certificates.com).

In het verlengde van het voorstel in Sectie 3.2 dat de internet stem beheersorganisatie de ISO 27001 standaard adopteert, stellen wij voor dat deze organisatie ook gecertificeerd wordt tegen deze standaard waarbij dit certificaat ook wordt gepubliceerd (bijvoorbeeld op de website van deze organisatie). Deze certificering moet gezien worden als een basis; aanvullende aandacht van een auditor moet uitgaan naar de beveiligingskritische onderdelen van het internetstemproces zoals bijvoorbeeld:

- De zorgvuldige inproductiename van het internetstemsysteem ('installatie') en de vaststelling dat dit systeem correspondeert met het systeem waar een andere auditor een verklaring over heeft afgegeven (zie het volgende punt).
- De kwaliteit van de onafhankelijke waarneming en verslaggeving daarvan tijdens het stemproces.

Wat deze beveiligingskritische onderdelen zijn, moet naar voren komen in de risico analyse die centraal staat bij de ISO 27001 standaard. De aandacht van een auditor naar deze beveiligingskritische onderdelen moet zijn vastgelegd in een audit plan aanvullend op het ISO 27001 certificering audit plan. Daarin moet ook zijn vastgelegd over welke aspecten de auditor aanvullende verklaringen af moet geven (bijvoorbeeld over de zorgvuldige inproductiename van het internetstemsysteem). Voor additionele onderbouwing kan de stem-beheersorganisatie ook een selectie van de onderliggende documentatie publiceren zoals bijvoorbeeld de centrale risico-analyse en de Statement of Applicability.

4.2 Publieke onderbouwing betrouwbaarheid internetstemsysteem

In Sectie 3.3 hebben wij voorgesteld de borging van informatiebeveiliging in de software levencyclus (ontwikkeling, onderhoud) van het internetstemsysteem minimaal te laten voldoen aan de NIST standaard SP 800-64 [9.]. Daarbij hebben wij voorgesteld te onderzoeken of ook andere standaarden moeten worden opgelegd.

In het verlengde hiervan stellen wij voor dat een onafhankelijke auditor (aangewezen door de Kiesraad) een onderzoek uitvoert naar de toepassing van de geadopteerde standaarden rond informatiebeveiliging (waaronder dus de NIST standaard) binnen de softwareontwikkelcyclus van het internetstemsysteem en hierover een publieke mededeling afgeeft. Daarbij dienen deze onderzoeken periodiek te worden herhaald en dienen bij grote veranderingen in het internetsysteem specifieke onderzoeken te worden uitgevoerd. Voor additionele onderbouwing voor de betrouwbaarheid van het internetsysteem kan ook een selectie van de onderliggende documentatie worden gepubliceerd (documenten voorgeschreven in de NIST 800-64 standaard zoals bijvoorbeeld risico analyses en de opzet van de gekozen maatregelen) alsmede (delen van) de broncode van het internet systeem.

5. Referenties

[1.] "Stemmen van vertrouwen", Adviescommissie inrichting verkiezingsproces, 27 september 2007.

[2.] "Information technology — Security techniques — Information security management systems — Requirements", ISO 27001, versie 2005-10-18.

[3.] "Information technology — Security techniques — Code of practice for information security management", ISO 27002, versie 2005-06-15.

[4.] "Information security management systems - Part 3: Guidelines for information security risk management", BS7799-3, maart 2006 (deze standaard wordt geadopteerd als ISO 27003).

[5.] "Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems", ISO 27006, 2007-03-01

[6.] "Control Objectives for Information and related Technology", ISACA, versie 4.1, zie www.isaca.org.

[7.] "Information Technology Infrastructure Library", http://www.itsmf.com.

[8.] "Information technology - Software life cycle processes", ISO 12207, versie 2004-11-12.

[9.] 'Security Considerations in the Information System Development Life Cycle', NIST special publication 800-64, juni 2004. Zie http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf.

[10.] "Evaluation criteria for IT security", ISO 15408, versie 2005-10-01, zie http://isotc.iso.org.

[11.] "Schema voor Certificatie van Informatiebeveiliging op basis van ISO/IEC 27001", ECP.NL, versie 4.0. Zie http://www.ecp.nl.

6. De ISO 27001 standaard

De ISO 27001 standaard getiteld 'Information Security Management Systems Requirements' [2.] beschrijft een management system voor informatiebeveiliging dat vergelijkbaar is met het management systeem voor kwaliteit beschreven in ISO 9001. Dit systeem dat Information Security Management System (hierna: ISMS) heet, heeft als doel dat op systematische en adequate wijze beveiligingsmaatregelen ('controls') worden toegepast. Deze beveiligingsmaatregelen staan in belangrijke mate beschreven in een andere ISO standaard (ISO 27002, zie [3.]) getiteld 'Code of practice for information security management' die gezien kan worden als een verzamelplaats van allerhande typen beveiligingsmaatregelen. De ISO 17799 omvat 11 hoofdstukken met beschrijvingen van beveiligingsmaatregelen op de verschillende terreinen:

H	ISO 27002	Nederlandse Vertaling (NEN)
5	Security Policy	Beveiligingsbeleid
6	Organization of Information Security	Beveiligingsorganisatie
7	Asset Management	Classificatie en beheer van bedrijfsmiddelen
8	Human resources security	Beveiligingseisen ten aanzien van personeel
9	Physical and Environmental Security	Fysieke beveiliging en beveiliging van de omgeving
10	Communications and Operations Management	Beheer van communicatie- en bedieningsprocessen
11	Access Control	Toegangsbeveiliging
12	Information Systems Acquisition, Development and Maintenance	Ontwikkeling en onderhoud van systemen
13	Information Security Incident Management	Incidentmanagement
14	Business Continuity Management	Continuïteitsmanagement (Business Continuity Management)
15	Compliance	Naleving

Centraal binnen het ISMS is een zogenaamde 'Plan'-, 'Do'-, 'Check'- en 'Act'-cyclus (PDCA) voor informatiebeveiliging. In de 'Plan'-fase worden door de organisatie plannen gemaakt die in de 'Do-fasen worden geïmplementeerd, in de 'Check'-fase wordt de implementatie periodiek beoordeeld en in de 'Act'-fase worden periodiek veranderingen gepland in het ISMS waardoor de cyclus weer bij de 'Plan'-fase start. ISO 27001 beschrijft specifieke eisen die worden gesteld aan deze generieke PDCA cyclus in de context van informatiebeveiliging. Het gebied waarover het ISMS 'gaat' heet de *scope* van het ISMS.

De ISO 27001 standaard schrijft de volgende eisen in hoofdlijn voor, onderscheiden naar: Algemeen, Plan, Do, Check en Act.

Algemene eisen

1. Centraal management proces rond informatiebeveiliging.
   Er dient een centraal management proces te zijn dat toeziet dat de PDCA cyclus consequent wordt gevolgd door de organisatie. Dit betekent ook dat het (senior) management actief deel uitmaakt van het proces en ook zorgt dat voldoende mensen en financiële middelen beschikbaar zijn. Het centrale managementproces dient voldoende geformaliseerd en gedocumenteerd te zijn bijvoorbeeld in een informatiebeveiligingsbeleid.

2. Centraal documentatie systeem.
   Er dient een documentatiesysteem te zijn waarin alle relevante documentatie (beleidsdocumenten, beveiligingsplannen en beveiligingsprocedures) is vastgelegd of eenduidig naar wordt gerefereerd. De bedoeling is dat alle personen werkzaam binnen de *scope* van het ISMS op efficiënte wijze beschikking kunnen krijgen over de relevante, actuele informatie over informatiebeveiliging. Impliciet voor het documentatiesysteem is daarom een autorisatie raamwerk waarmee eenduidig vastgesteld kan worden dat een document van toepassing is ('geautoriseerd') en een versiesysteem waarmee vastgesteld kan worden dat een document actueel is.
3. Centrale registratie informatiesystemen ('assets').
   Er dient een centrale registratie te zijn van alle informatiesystemen ('assets') die zich bevinden binnen de *scope* van het ISMS. Daarbij dient ook de verantwoordelijkheid voor de informatiesystemen vastgelegd te zijn.

Eisen aan de Plan-fase

4. Risicoanalyse methode.
   Er dient een Risicoanalyse methode te zijn vastgelegd/ontwikkeld (vergelijk [4.]) die toegepast op informatiesystemen dient te worden die zich binnen de scope van het ISMS bevinden. De Risicoanalyse methode dient de volgende zaken op systematische wijze te adresseren:
   - Analyse van risico's waar het informatiesysteem aan bloot staat op basis van een analyse van bedreigingen, kwetsbaarheden, gevolgen en waarschijnlijkheden van optreden. Het betreft hier niet alleen ICT-risico's, maar nadrukkelijk ook risico's die afkomstig zijn uit de bedrijfsprocessen die gebruik maken van het informatie systeem. Het is daarom van belang dat bij de analyse van deze risico's vertegenwoordigers van verschillende disciplines (met name bedrijfsprocessen en ICT) betrokken zijn. Vergelijk [4.].
   - Analyse van maatregelen of verzamelingen van maatregelen om deze risico's te beperken, te vermijden of elders neer te leggen (bijvoorbeeld middels verzekeringen).
   - Keuze en vastlegging van een maatregel set op basis van acceptabele rest risico's. Daarbij dient gemotiveerd te worden waarom een bepaalde maatregel uit ISO 17799 niet wordt overgenomen.
5. Toepassing van de Risicoanalyse methode.
   De Risicoanalyse methode dient consequent te worden toegepast per onderscheiden informatiesysteem binnen de *scope* van het ISMS uitmondend in een zogenaamde *statement of applicability* (per informatiesysteem of overkoepelend). Duidelijk dient gemaakt te kunnen worden dat de opzet van de getroffen maatregelen de onderscheiden risico's voldoende adresseren. Overigens betekent dit niet noodzakelijk dat voor alle informatiesystemen een gedetailleerd risicoanalyse hoeft te worden uitgevoerd. Vrij gebruikelijk is de toepassing van een twee-traps-methode (*'combined approach'*). In de eerste trap wordt met een eenvoudige methode bepaald of een systeem 'bedrijfskritisch' is of niet. Indien dit niet het geval is, wordt volstaan met een generieke baseline van maatregelen. Indien een systeem wel bedrijfskritisch is wordt een specifieke risicoanalyse uitgevoerd. Voorbeelden van een dergelijke methoden zijn SPRINT/SARA/IRAM ontwikkeld door het Information Security Forum (www.securityforum.org).

Eisen aan de Do fase

6. Implementatie van beveiligingsmaatregelen en effectiviteitcriteria.
   De vastgelegde beveiligingsmaatregelen dienen te worden geïmplementeerd. Hiervoor moet een informatiebeveiligingsplan (*risk treatment plan*) worden opgesteld. Er dient daarbij te worden vastgelegd hoe bepaald gaat worden dat beveiligingsmaatregelen effectief zijn. Essentieel hierbij is ook de realisatie van een proces waarin beveiligingsincidenten binnen het ISMS kunnen worden gemeld, vastgelegd, opgevolgd en geanalyseerd.

Eisen aan de Check-fase

7. Monitor de geïmplementeerde beveiligingsmaatregelen en de totstandkoming daarvan.
   Dit kan bijvoorbeeld middels:
   - Rapportages over effectiviteit van maatregelen tegen de vastgelegde effectiviteit criteria.
   - Rapportages over beveiligingsincidenten.
   - Audits van interne of externe aard.

Eisen aan de Act fase

8 Verbetering van het ISMS.

Aan de hand van resultaten van de 'Check'-fase wordt het ISMS verbeterd. Dit kan bijvoorbeeld betekenen dat het informatiebeveiligingsbeleid veranderd, dat de risicoanalyse methode moet worden aangepast of dat bepaalde maatregelen anders moeten worden geïmplementeerd.