Round Table ISO27001:2013

5 mei 2014

Agenda

- Introductie
- Samenvatting certificering
- ISO27001:2005 versus ISO27001:2013
  - Wat is er veranderd?
  - Wat zijn de consequenties?
  - Wat zijn de eerste ervaringen met de nieuwe ISO?
- Afsluiting

Introductie

- Drs. Pier Nauta RE CISSP CISA
- Vidar Security
- Track record:
  - Deloitte & Touche
  - IB-Groep (tegenwoordig DUO)
  - Ordina
  - PwC
  - Freelance

www.vidar-security.nl

www.linkedin.com/in/piernauta

@piernauta1

+316 2557 1569

Vooraf

- Graag telefoons uit/stil
- Alleen de opvallende verschillen tussen 2005 en 2013 versie
- Niet gestreefd naar volledigheid
- Tempo zal hoog liggen
- Vragen tussendoor zijn welkom
- Schaf de ISO27001:2013 aan
- Bestudeer de nieuwe versie goed (voordat je aan de slag gaat)
- Sheets worden later verstrekt

Achtergrond Certificering

ISO27001:2013 certificering

- Audit van het management systeem van organisatie
- Organisatie moet voldoen aan specifieke eisen
- Door externe geaccrediteerde partij
- Op basis van objectief bewijs

- Opzet, bestaan en werking

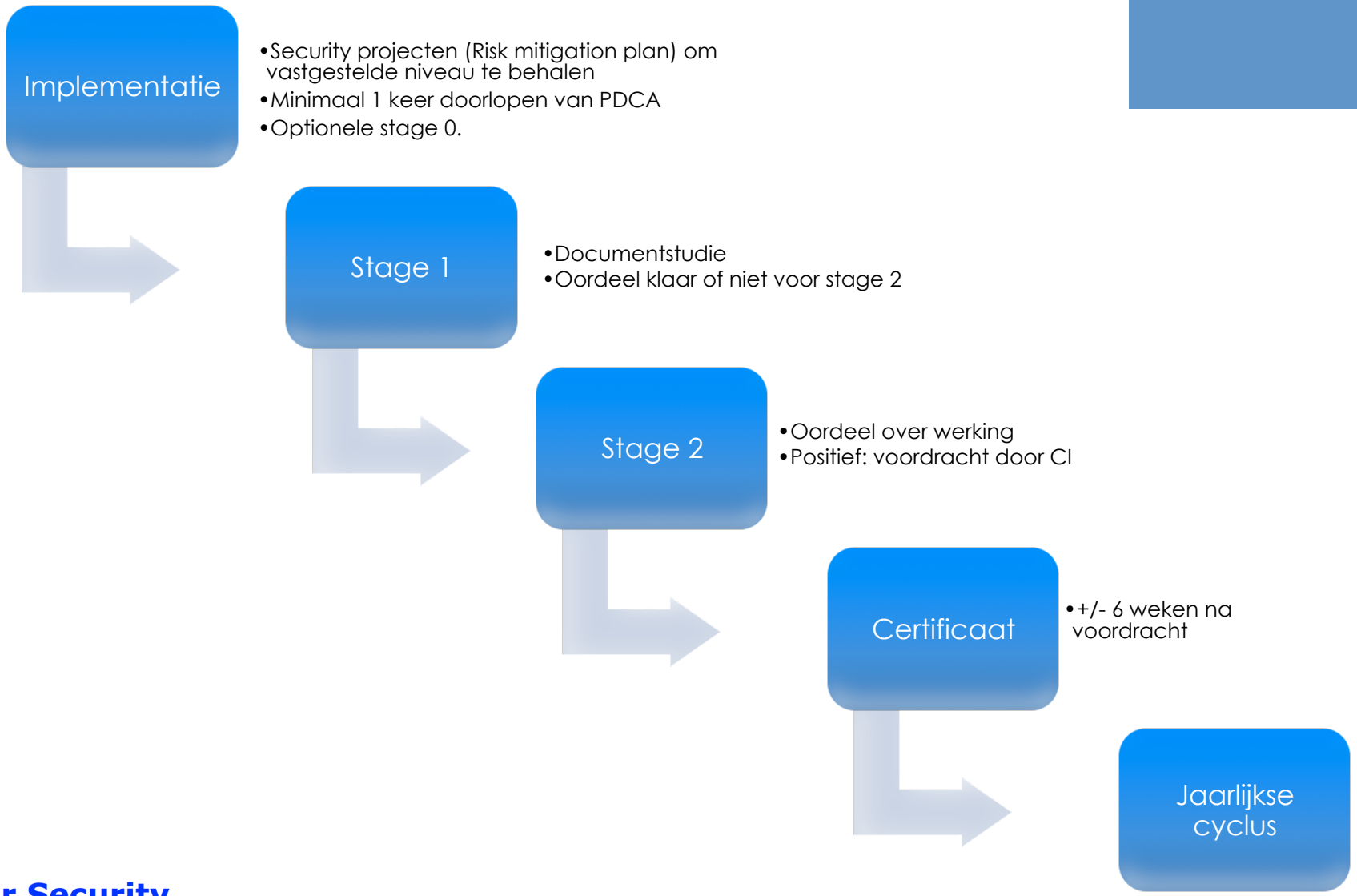
ISO27001:2013 certificering

- Bepalen wat het gewenste / noodzakelijk niveau van informatiebeveiliging is
- Opschrijven wat je doet om dat niveau:
  - te bereiken
  - te behouden
  - te verbeteren
- Aantoonbaar maken dat gedaan wordt wat is opgesteld

ISO27001:2013 certificering

- Nooit 100% beveiligd
- Geen garantie dat je nooit meer incidenten krijgt
- Geen uitspraak over technische inrichting
- Geen papieren exercitie (gaat om werking)
- Geen "one size fits all"
- Geen ontslag van verantwoordelijkheid bij outsourcing

Certificeringsproces



Cyclus

Jaar 1
- Initiële audit

Jaar 2
- Tussentijdse audit

Jaar 3
- Tussentijdse audit

Jaar 4
- Nieuwe volledige cyclus

- Driejarige cyclus
- Blijvend voldoen aan de criteria
- Aantoonbaar doorlopen van ISMS
- Aantoonbare continue verbetering

Overview

ISO27001:2013 achtergrond

- Vorige versie is 8 jaar oud
- Release was verrassing
  (2 maanden eerder dan initieel aangekondigd)
- Herziening noodzakelijk
- Behoefte om meer aan te sluiten bij overige ISO standaarden

Vooruitlopend

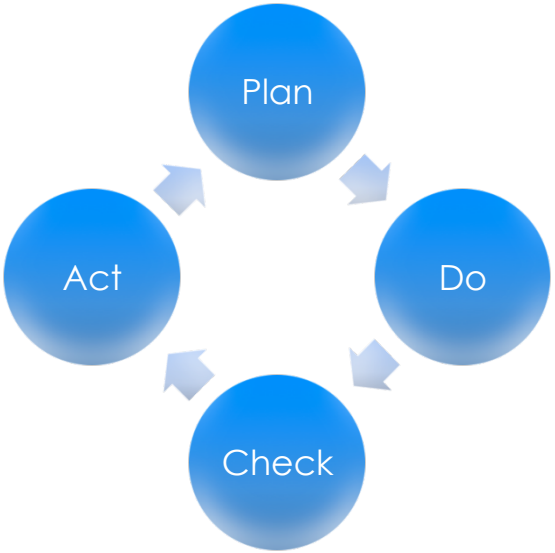
- Aangepast aan een modernere context
- De norm is feitelijk geheel herschreven
  - Volgorde
  - Taalgebruik
- Aansluiting bij overige ISO normen
- Aantal fundamentele zwakheden zijn opgelost
- Aantal nieuwe zwakheden zijn geïntroduceerd
- Geeft meer vrijheid aan organisaties
- Eist meer tijdens implementatie
- Eist meer van de auditor

Niet alles is veranderd

- De essentie blijft informatiebeveiliging
  - Beschikbaarheid
  - Integriteit
  - Vertrouwelijkheid
- Nog steeds generiek
- Het audittraject blijft hetzelfde

Overeenkomst

- Deming Cycle
- In 2005-versie nog expliciet (0.2)
- In 2013-versie impliciet



Aandacht

- ISO27001 opgebouwd uit Clauses en Annex A
- Clauses hebben betrekking op ISMS
- Annex A best practices

Verschil tussen:

- Shall
- Should

Verschillen clauses

Indeling

ISO27001:2005

4: Information Security Management System

5: Management Responsibility

6: Internal ISMS Audits

7: Management Review of the ISMS

8: ISMS Improvement

ISO27001:2013

4: Context of the Organization

5: Leadership

6: Planning

7: Support

8: Operation

9: Performance Evaluation

10: Improvement

Wijzigingen in de clauses

- Volgorde
- 21 eisen zijn verwijderd (bijlage 1 en 2)
- 32 nieuwe eisen aan het ISMS (bijlage 3 en 4)
- Significante wijzigingen in formulering

Indeling

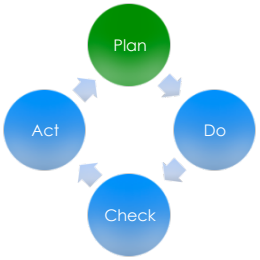
	ISO27001:2013
Plan	4: Context of the organization
	5: Leadership
	6: Planning
	7: Support
Do	8: Operation
Check	9: Performance evaluation
Act	10: Improvement

Clauses

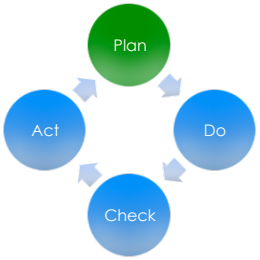
- Clause 0. Introduction
  - De sectie over PDCA is verwijderd
- Clause 1. Scope
  - Geen opmerking meer over uitsluiting van controls in annex A.
- Clause 2. Normative references
  - Alleen verwijzing naar 27000
- Clause 3. Terms and definitions
  - Is er niet meer.
  - Alleen verwijzing naar 27000

4. Context of the organization

- Nieuwe clause
- Vangt deels het verwijderen van preventive actions op
  - Issues
  - Risks
  - Opportunities
- Explicieter rekening houden met omgeving
  - Tegemoetkoming aan netwerkorganisaties?



4. Context of the organization



Nieuw zijn twee eisen:

1. Determine interested parties
2. Their requirements

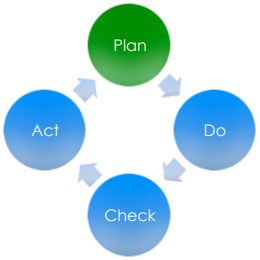
Opvallend:

Interested parties vs stakeholders

4. Context of the organization

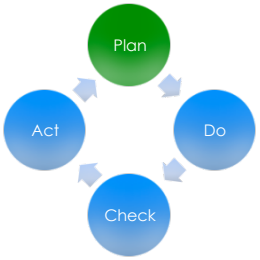
- Opgelost door grafische weergave
- Per relatie aangegeven:
  - Specifieke wettelijke bepalingen
  - Specifieke eisen
  - Specifieke afspraken
  - Informatiestromen
  - Classificatie
  - Afspraken Rapportage
  - Afspraken (verwijzingen) relevant
  - etc

5. Leadership



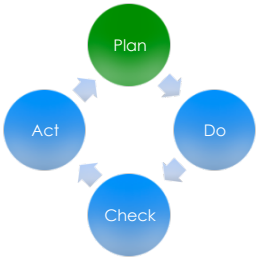
- Direct opvallend is introductie van de term: “top management”
  - Daarmee wordt hoogste level bedoeld
  - Binnen (het deel van) de organisatie waarvoor het certificaat geldt
- Focus op vaststellen policy
- Verdelen van taken, bevoegdheden en verantwoordelijkheden
- Focus op commitment
- Focus op continue verbetering
- Delegeren kan…. Mits!

6. Planning



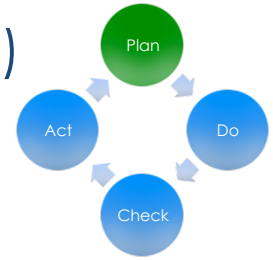
- Aantal fundamentele wijzigingen
- Waar 2005 versie uitging van de assets tbv risico assessment, is er nu verschuiving naar de asset "information"
  - Bijvoorbeeld: in 2005 versie moesten de laptops als asset worden geïdentificeerd en daar dan de risico analyse op uitvoeren.
    In 2013 versie betreft het de informatie op eventueel de laptops (of cloud)
- Benoeming van risk owners (ipv asset owners)
- Modernisering en meer to-the-point
- Risk assessment deel is uitgebreider en neigt naar een meer kwantitatieve insteek

6. Planning



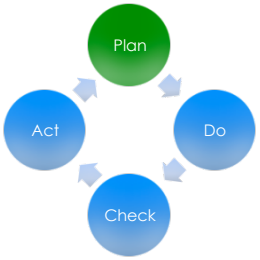
- Er wordt nu echter gesproken over: determination (vaststellen) of controls
- 6.1.3 (b) Note: Organizations can design controls as required, or identify them from <u>any source</u>. (meer informatie bij sheets over Annex A)
- Annex A = CHECK LIST
- Ieder willekeurig security framework mag gebruikt worden
  - Bijvoorbeeld Cobit
  - Bijvoorbeeld NIST

6. Planning



- Nog steeds opstellen Statement of Applicability (SOA)
  - Hoe dan?
- Kan problemen opleveren
  - Zeker voor grotere complexere organisaties
- Opgelost door: De annex A als SOA te gebruiken.

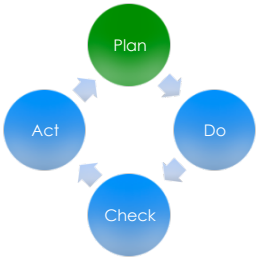
7. Support



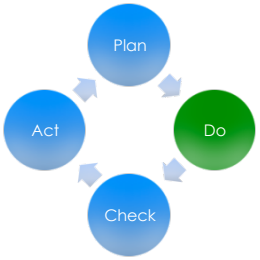
- Begint met eis dat de organisatie de benodigde resources:
  - Vaststelt en
  - Vrijmaakt
- Om het ISMS:
  - Te implementeren
  - Te onderhouden
  - Continu te verbeteren
- Stelt eisen aan competenties, awareness en communication

7. Support

- Introductie van nieuwe term: “documented information”
- Vervangt:
  - Documents
  - Records
- **NB**: afzonderlijke paragrafen geven nu aan dat er documented information moet zijn



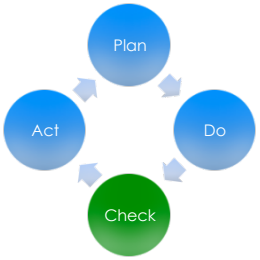
8. Operation



- Uitvoeren wat tot nu toe aan clauses wordt geëist
- Periodiek risk assessment uitvoeren
- Uitvoeren van risk treatment plan

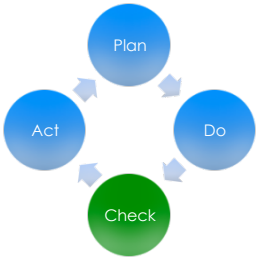
- Met andere woorden: houd het ISMS draaiende

9. Performance evaluation



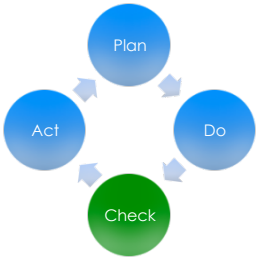
- Algemeen: bepaal welke informatie geëvalueerd moet worden om:
  - Informatiebeveiliging te evalueren
  - Effectiviteit ISMS vast te stellen
- Doel is bepaling van nodige informatie ipv wat de organisatie kan evalueren
  - In het kader van de efficiency
  - "The methods selected should produce comparable and reproducible results to be considered valid."
- Wordt aangeraden meting aan te passen aan doelstellingen, tijd en volwassenheidsniveau

9. Performance evaluation



- Internal audit is vrijwel identiek aan de 2005-versie
- “without due delay” is verwijderd
  - (maar komt terug in clause 10)
- In 2005 versie stond dat auditoren hun eigen werk niet mogen auditen.
- In 2013 vervangen door eisen ten aanzien objectiviteit en onpartijdigheid

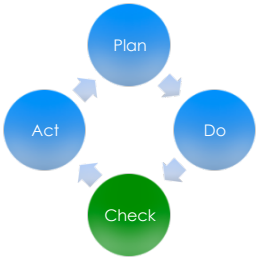
9. Performance evaluation



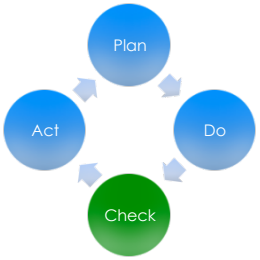
- Grootste wijziging betreft de Management review
- Geen specifieke eisen meer ten aanzien van:
  - Input
  - Output
- Vervangen door onderwerpen (considerations)

9. Performance evaluation

- 9.3 Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness
- Dus niet meer minimaal eens per jaar



9. Performance evaluation

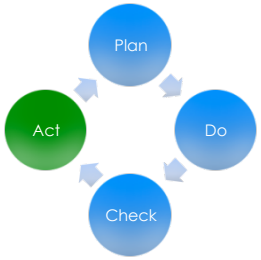


- Gevolg (mijns inziens) kan op termijn leiden tot minder commitment vanuit top management

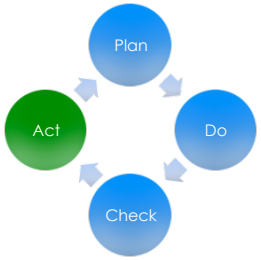
- Implementatie: toch minimaal eens per jaar.
  - Vastleggen in beleid en procedures
  - Inbedden in cyclus
  - Vaker bij hoger risicoprofiel

10. Improvement

- Niet langer ISMS improvement
- 2005 versie sprak over preventative and corrective actions
- 2013 versie alleen over corrective actions
- Nog steeds sprake van determine root cause



10. Improvement



- Reageren op non conformiteit en actie ondernemen
- Vaststellen of er vergelijkbare non-conformiteiten zijn
  - (Preventive action?)
- Nieuwe eis: correctieve actie moet PASSEND zijn
- Nieuwe eis: continue verbetering uitgebreid naar:
  - Suitability of ISMS
  - Adequacy of ISMS

Documented information

Verplichte documenten & records

- Erg belangrijk gedurende de audit
  - Harde eisen
  - Aantoonbaarheid
- Altijd veel discussie
- Uitbreiding van verplichte documenten
- Explicietere benoeming van records

Verplichte documenten

- In 2005-versie slechts op 4 plekken verplichte beschreven procedures benoemd (documented procedures):
  - Document control (4.3.2)
  - Internal audits (6)
  - Corrective actions (8.2)
  - Preventive actions (8.3)

Documented information

- De term “documented procedure” komt niet meer terug in de 2013 versie
- Is nu “documented information”
- Komt op veel meer plekken terug
  - Clauses
  - Annex A
- Voorbeelden:
  - Procedures
  - Procesbeschrijvingen
  - Records / archief
  - Notulen
  - …
- Bijlage 9, 10, 11 en 12

Verplichte records

- ISO27001:2005 4.3.3.
- Verwijderd:
  - The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.
  - …and of all occurrences of significant security incidents related to the ISMS.

Verplichte records

- Gesplitst naar:
  - adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity) (7.5.3 (b)
  - storage and preservation, including the preservation of legibility (7.5.3 (d))
  - be available as documented information (5.2 (c))
  - ensuring that the information security management system conforms to the requirements of this International Standard (5.3 (a))
  - reporting on the performance of the information security management system to top management (5.3 (b))
  - The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned (8.1)
  - The organization shall retain documented information of the results of the information security risk assessments. (8.2)
  - retain documented information as evidence of the audit programme(s) and the audit results (9.2 (g))

Verplichte records

- Concreet:
  - Records of training, skills, experience and qualifications
  - Monitoring and measurement results
  - Internal audit program
  - Results of internal audits
  - Results of the management review
  - Results of corrective actions
  - Logs of user activities, exceptions, and security events

Gevolgen

- Meer vrijheid = meer verantwoordelijkheid
- Meer principe georiënteerd

- Meer eisen aan implementator
  - Vereist meer kennis en kunde
  - Moet passend zijn
  - Geen standaard implementaties meer
  - Tooling is niet praktisch
- Meer eisen aan auditor
  - De “vinkenlijst” is abstracter
  - Moet zich nog meer in de situatie van organisatie verplaatsen

Verschillen Annex A

De Annex A

- Van 133 naar 114 controls
- 20 controls verwijderd (Bijlage 5 en 6)
- 11 nieuwe controls (Bijlage 7 en 8)

- ISO27001 is nog steeds de enige norm met een Annex A
- De functie van Annex A is gewijzigd

Annex A niet meer verplicht

6.1.3 (c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted

Notes:

1. Annex A contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A to ensure that no necessary controls are overlooked.

2. Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may be needed.

Wat betekent dit?

- Waarschijnlijk meest ingrijpende wijziging
- Ieder willekeurig security framework mag gebruikt worden
  - Bijvoorbeeld Cobit
  - Bijvoorbeeld NIST
- Mits: deze voldoet aan de controls in annex A
- Tegenstrijdigheid in notes vereist meer van implementatie en auditoren
- Lastiger om een Statement of applicability te maken

De Annex A

- Best practices
- Geen “one size fits all”
- Vertalen naar specifieke context organisatie

De Annex A

5. Security policy

6. Organization of information security

7. Asset management

8. Human resources security

9. Physical and enviromental security

10. Communications and operations management

11. Access control

12. Information systems acquisition, development and maintenance

13. Information Security Incident Management

14. Business Continuity Management

15. Compliance

5. Information Security policies

6. Organization of information Security

7. Human resource security

8. Asset management

9. Access control

10. Cryptography

11. Physical and environmental security

12. Operations Security

13. Communications Security

14. Systems acquisition, development and maintenance

15. Supplier relationships

16. Information Security Incident Management

17. Information Security aspects of business continuity

18. Compliance

Nieuwe hoofdstukken

De Annex A ISO27001:2013

5. Information Security policies

6. Organization of information Security

7. Human resource security

8. Asset management

9. Access control

10. Cryptography

11. Physical and environmental security

12. Operations Security

13. Communications Security

14. Systems acquisition, development and maintenance

15. Supplier relationships

16. Information Security Incident Management

17. Information Security aspects of business continuity

18. Compliacnce

De verwijderde controls ISO27001:2005

- Overzicht van verwijderde controls in Bijlage 6
- Te vinden in:
  - A6 (Organization of information security)
  - A10 (Communications and operations management)
  - A11 (Access control)
  - A12 (Information systems acquisition, development and maintenance)
  - A15 (Compliance)

De verwijderde controls ISO27001:2005

- Verwijderde controls uit A6 zijn naar clauses verhuisd.
  - Commitment
  - Context van organisatie
- Zijn naar de clauses “gepromoveerd”

De verwijderde controls ISO27001:2005

- A10.10.1; A10.10.2; A10.10.5 (logging) verwijderd
- Zijn gegroepeerd in: A12.4.1
- Interessant: nieuwe term is event logging
  - Positievere connotatie

De verwijderde controls ISO27001:2005

- A11.6.2 Sensitive System Isolation
- Verwijderd vanuit de gedachte dat dit een overbodige control is in een “connected world”
- Indien organisatie deze control wel nodig acht, kan deze of soortgelijke wel teruggebracht worden

De verwijderde controls ISO27001:2005

- Verwijderde controls (A12) vallen onder de noemer: correct processing in applications
  - Input, output, validation,
  - authenticity
- Logisch dat deze is verwijderd
- Wordt vervangen door het concept “security by design”

De verwijderde controls ISO27001:2005

- A15.1.5 .. deterence of unautorized use …
- A15.3.2 … access to information systems to prevent misuse …
- De eisen uit A15 (Compliance) die verwijderd zijn eveneens niet echt verwijderd.
- Komen niet meer letterlijk terug, maar wel op een meer principieel niveau

De verwijderde controls ISO27001:2005

- Dus eigenlijk is er niet zoveel verwijderd
- En wat verwijderd is, op een hoger (abstractie) niveau getild, of
- Kan op basis van eigen inzicht weer terugkomen

De nieuwe controls ISO27001:2013

- Bijlage 7 & 8
- Zijn abstract en nog steeds op principe niveau
- Vertaling is afhankelijk van context organisatie

De nieuwe controls ISO27001:2013

Even stil staan bij paar interessante aspecten uit nieuwe controls:

- Security by design
- BCM

Security by design

- Vorige versies kwam dit nog niet duidelijk terug
- Op meerdere plekken komt dit principe terug
  - Development, acquisition, BCM, policies
  - Komt op principe niveau door hele code terug
- Nu is het grootste deel van A14 eraan gewijd
  - Totaal 13 controls!
- "Secure systems engineering principles"
  - Documented information

Security by design

- Mijn opvatting: grote sprong voorwaarts
- Zal enorme kwaliteitsverbetering tot gevolg hebben

- Het achteraf repareren levert veel issues op
- Soms erger dan oorspronkelijke probleem
  - Achteraf een kreukelzone in een auto inbouwen is ook lastig

A17 Information Security aspects of business continuity

- 2005 versie was het: A14. Business Continuity Management
- Van 5 naar 4 controls
- Heel A14(2005) op abstract niveau wordt samengevat in
  - A17.1.1
  - A17.1.2
  - A17.1.3
- Terwijl de A17.2.1 (redundancies) de enige meer operationele control is

A17 Information Security aspects of business continuity

- Door deze formulering is het feitelijk een verwijzing naar ISO22301?
- Lijkt het wel op
  - Hoger abstractie niveau
  - Gelijkschakeling inhoudsopgave

ISO27001 en NEN7510

Relatie NEN7510

- Voor organisaties die zowel ISO27001 en NEN7510 certificaat hebben of daar naar streven
- Huidige NEN7510 = ISO27001:2005 + ISO27002 + 23 additionele normen mbt patiëntgegevens
- De aansluiting is niet meer eenduidig
- Onduidelijk hoe NEN hiermee zal gaan

Relatie NEN7510

- Beste geval: meer gelijkschakeling + reparatie onduidelijkheden
- Ergste geval: verder uiteenlopen
- Vergt nieuwe strategie voor organisaties die beide certificaten willen

Afsluitend

Vervolg

- Tot half jaar na release ISO27001:2013 kan nog tegen ISO27001:2005 worden gecertificeerd
- Binnen twee jaar (oktober 2015) na release moet gehercertificeerd zijn tegen nieuwe norm

Advies

- Bij nieuwe certificering: direct nieuwe norm hanteren
- Bij bestaande certificering:
  - Schaf nieuwe norm aan
  - Maak deze zo snel mogelijk eigen
  - Inplannen
  - Volledige inventarisatie
  - Bepaal strategie
    - Quick fix
    - Volledige herinterpretatie

Strategieën

- Initiële audit
- Transitie
  - Quick fixes
  - Volledige herinterpretatie

Uitdagingen

- Issues (4.1 en 6.1.1)
- Risk and opportunities (4.1 4.2)
- Monitoring, measurement, analysis and evaluation (9.1)
- Statement of applicability

Overige aandachtspunten

- Documented information
- Policy
- Risk assessment
- Control of documentation
- Improvement
- Corrective actions
- Management review
- Awareness
- Internal audit

Conclusie

Conclusie

- Aangepast aan een meer moderne context
- De norm is feitelijk geheel herschreven
  - Volgorde
  - Taalgebruik
- Aansluiting bij overige ISO normen
- Aantal fundamentele zwakheden zijn opgelost
- Aantal nieuwe zwakheden zijn geïntroduceerd
- Geeft meer vrijheid aan organisaties
- Eist meer tijdens implementatie
- Eist meer van de auditor

www.vidar-security.nl

www.linkedin.com/in/piernauta

@piernauta1

+316 2557 1569

Bijlagen

Informatie

- Het is ten zeerste aanbevolen om ISO27001:2013 aan te schaffen via de reguliere kanalen
- De ISO27001:2013 dient goed bestudeerd te worden vooraf gaand aan een succesvolle implementatie
- De hier verstrekte bijlagen zijn indicatief
- Voor de verstrekte bijlagen geldt geen garantie op volledigheid
- De genoemde clauses en controls an sich zijn niet voldoende om een functionerend ISMS in te richten. De clauses en controls moeten in samenhang worden gezien met de overige maatregelen in de ISO27001:2013
- Gebruik van de bijlagen voor welk doel dan ook is voor eigen risico

Bijlage 1.Overzicht verwijderde clauses

- 4.2.1 (g)
- 4.2.1 (i)
- 4.2.3 (a)(1)
- 4.2.3 (a)(2)
- 4.2.3 (a)(4)
- 4.2.3 (a)(5)
- 4.2.3 (h)
- 4.3.1
- 4.3.1
- 4.3.1 (c)
- 4.3.2
- 4.3.3
- 4.3.3
- 5.2.1 (b)
- 5.2.1 (d)
- 6(d)
- 8.2
- 8.3
- 8.3 (d)
- 8.3 (e)
- 8.3 (e)

Bijlage 2. Verwijderde clauses (1)

4.2.1 (g) Select control objectives and controls for the treatment of risks. (red. Uit annex A)

4.2.1 (i) Obtain management authorization to implement and operate the ISMS.

4.2.3 Execute monitoring and reviewing procedures and other controls to:

4.2.3 (a)(1) promptly detect errors in the results of processing

4.2.3 (a)(2) promptly identify attempted and successful security breaches and incidents

4.2.3 (a)(4) help detect security events and thereby prevent security incidents by the use of indicators; and

4.2.3 (a)(5) determine whether the actions taken to resolve a breach of security were effective.

4.2.3 (h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3)

Bijlage 2. Verwijderde clauses (2)

4.3.1 Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and ensure that the recorded results are reproducible.

4.3.1 It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.

4.3.1 (c) (The ISMS documentation shall include) procedures and controls in support of the ISMS;

4.3.2 A documented procedure shall be established to define the management actions …

4.3.3 The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.

4.3.3 … and of all occurrences of significant security incidents related to the ISMS.

Bijlage 2. Verwijderde clauses (3)

5.2.1 (b)	ensure that information security procedures support the business requirements;
5.2.1 (d)	maintain adequate security by correct application of all implemented controls;
6(d)	(The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS) perform as expected
8.2	The documented procedure for corrective action
8.3	The documented procedure for preventive action shall define requirements for:
8.3 (d)	recording results of action taken (see 4.3.3); and
8.3 (e)	reviewing of preventive action taken
8.3 (e)	The priority of preventive actions shall be determined based on the results of the risk assessment.

Bijlage 3. Overzicht nieuwe clauses

- 4.2 (a)
- 4.3 (c)
- 5.1 (b)
- 6.1.1 (a)
- 6.1.1 (b)
- 6.1.1 (c)
- 6.1.2 (a)
- 6.2 (b)
- 6.2 (c)
- 6.2 (c)
- 6.2 (f)
- 6.2 (g)
- 6.2 (h)
- 6.2 (i)
- 6.2 (k)
- 7.3 (a)
- 7.4 (a)
- 7.4 (b)
- 7.4 (c)
- 7.4 (d)
- 7.4 (e)
- 7.5.1 (b)
- 8.1
- 9.1 (c)
- 9.1 (d)
- 9.1 (f)
- 9.3 (c)(4)
- 10.1 (a)
- 10.1 (a)(1)
- 10.1 (a)(2)
- 10.1 (e)
- 10.1 (f)

Bijlage 4. Nieuwe clauses (1)

4.2 (a) The organization shall determine … interested parties that are relevant to the information security management system

4.3 (c) … consider… interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations

5.1 (b) ensuring the integration of the information security management system requirements into the organization's processes

6.1.1 (a) ensure the information security management system can achieve its intended outcome(s);

6.1.1 (b) prevent, or reduce, undesired effects;

6.1.1 (c) achieve continual improvement

6.1.2 (a) establishes and maintains information security risk criteria that include:
1) the risk acceptance criteria; and
2) criteria for performing information security risk assessments

Bijlage 4. Nieuwe clauses (2)

6.2 (b) (information security objectives shall) be measurable (if practicable);

6.2 (c) take into account applicable information security requirements, and results from risk assessment and risk treatment

6.2 (f) what will be done

6.2 (g) what resources will be required

6.2 (h) who will be responsible

6.2 (i) when it will be completed

6.2 (k) how the results will be evaluated

Bijlage 4. Nieuwe clauses (3)

7.3 (a)	(Persons doing work under the organization's control shall be aware of) the information security policy
7.4 (a)	(The organization shall determine the need for internal and external communications relevant to the information security management system including) on what to communicate
7.4 (b)	when to communicate
7.4 (c)	with whom to communicate
7.4 (d)	who shall communicate
7.4 (e)	the processes by which communication shall be effected
7.5.1 (b)	(ISMS shall include) documented information determined by the organization as being necessary for the effectiveness of the information security management system
8.1	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1

Bijlage 4. Nieuwe clauses (4)

9.1 (c) when the monitoring and measuring shall be performed

9.1 (d) who shall monitor and measure

9.1 (f) who shall analyse and evaluate these results

9.3 (c)(4) (feedback on the information security performance, including trends in) fulfilment of information security objectives

10.1 (a) react to the nonconformity, and as applicable:
1) take action to control and correct it; and
2) deal with the consequences;

10.1 (e) make changes to the information security management system, if necessary

10.1 (f) (documented information on) the nature of the nonconformities and any subsequent actions taken

Bijlage 5. Overzicht verwijderde controls ISO27001:2005

- A6.1.1
- A6.1.2.
- A6.1.4
- A6.2.1
- A6.2.2
- A10.7.4
- A10.8.5
- A11.4.2
- A11.4.2
- A11.4.3
- A11.4.4
- A11.4.6
- A11.4.7
- A11.6.2
- A12.2.1
- A12.2.2
- A12.2.3
- A12.2.4
- A12.5.4
- A15.1.5
- A15.3.2

Bijlage 6. Verwijderde controls ISO27001:2005 (1)

A6.1.1	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
A6.1.2.	Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.
A6.1.4	A management authorization process for new information processing facilities shall be defined and implemented.
A6.2.1	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
A6.2.2	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
A10.7.4	System documentation shall be protected against unauthorized access.
A10.8.5	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.

Bijlage 6. Verwijderde controls ISO27001:2005 (2)

A11.4.2 Appropriate authentication methods shall be used to control access by remote users.

A11.4.3 Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.

A11.4.4 Physical and logical access to diagnostic and configuration ports shall be controlled.

A11.4.6 For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).

A11.4.7 Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

A11.6.2 Sensitive systems shall have a dedicated (isolated) computing environment.

Bijlage 6. Verwijderde controls ISO27001:2005 (3)

A12.2.1	Data input to applications shall be validated to ensure that this data is correct and appropriate.
A12.2.2	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
A12.2.3	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
A12.2.4	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
A12.5.4	Opportunities for information leakage shall be prevented.
A15.1.5	Users shall be deterred from using information processing facilities for unauthorized purposes.
A15.3.2	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

Bijlage 7. Overzicht nieuwe controls ISO27001:2013

- A6.1.5
- A12.6.2
- A14.2.1
- A14.2.5
- A14.2.6
- A14.2.8
- A15.1.1
- A15.1.3
- A16.1.4
- A16.1.5.
- A17.2.1

Bijlage 8. Nieuwe controls ISO27001:2013 (1)

A6.1.5	Information security shall be addressed in project management, regardless of the type of the project
A12.6.2	Rules governing the installation of software by users shall be established and implemented.
A14.2.1	Rules for the development of software and systems shall be established and applied to developments within the organization.
A14.2.5	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.
A14.2.6	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.
A14.2.8	Testing of security functionality shall be carried out during development.

Bijlage 8. Nieuwe controls ISO27001:2013 (2)

A15.1.1 Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.

A15.1.3 Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

A16.1.4 Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

A16.1.5 Information security incidents shall be responded to in accordance with the documented procedures.

A17.2.1 Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Bijlage 9. Verplichte documenten ISO27001:2013

4.3.	Scope of ISMS
5.2. & 6.2	Information security policy and objectives
6.1.2	Risk assessment & risk treatment methodology
6.1.3	Statement of applicability
6.1.3 (e) & 6.2	Risk treatment plan
8.2	Risk assessment report

Bijlage 10. Verplichte documenten Annex A

A7.1.2 A13.2.4	Definition of security roles and responsibilities
A8.1.1	Inventory of assets
A8.1.3	Acceptable use of assets
A9.1.1	Access control policy
A12.1.1	Operation procedures for IT management
A14.2.5	Secure systems engineering principles
A15.1.1	Supplier security policy
A16.1.5	Incident management procedure
A17.1.2	Business continuity procedure
A18.1.1	Legal, regulatory and contractual requirements

Bijlage 11. Geadviseerd ISO27001:2013

7.5 Procedure for document control

7.5 Controls for managing records

9.2 Procedure for internal audit

10.1 Procedure for corrective actions

Bijlage 12. Geadviseerd Annex A (1)

A6.2.1	BYOD policy
A6.2.1	Mobile device and teleworking policy
A8.2.	Information classifcation policy
A9.2	Password policy
A8.3.2 A112.7	Disposal & destruction policy
A11.1.5	Procedure for working in secure areas
A11.2.9	Clean desk and clear screen policy

Bijlage 12. Geadviseerd Annex A (2)

A12.1.2 A14.2.4	Change management policy
A12.3.1	Backup policy
A13.2	Information transfer policy
A17.1.1	Business Impact Analysis
A17.1.3	Exercising and testing plan
A17.1.3	Maintenance and review plan
A17.2.1	Business continuity strategy

Bijlage 13. Records

- Records of training, skills, experience and qualifications
- Monitoring and measurement results
- Internal audit program
- Results of internal audits
- Results of the management review
- Results of corrective actions
- Logs of user activities, exceptions, and security events