Informatiebeveiliging
&
ISO/IEC 27001:2013

Aart Bitter

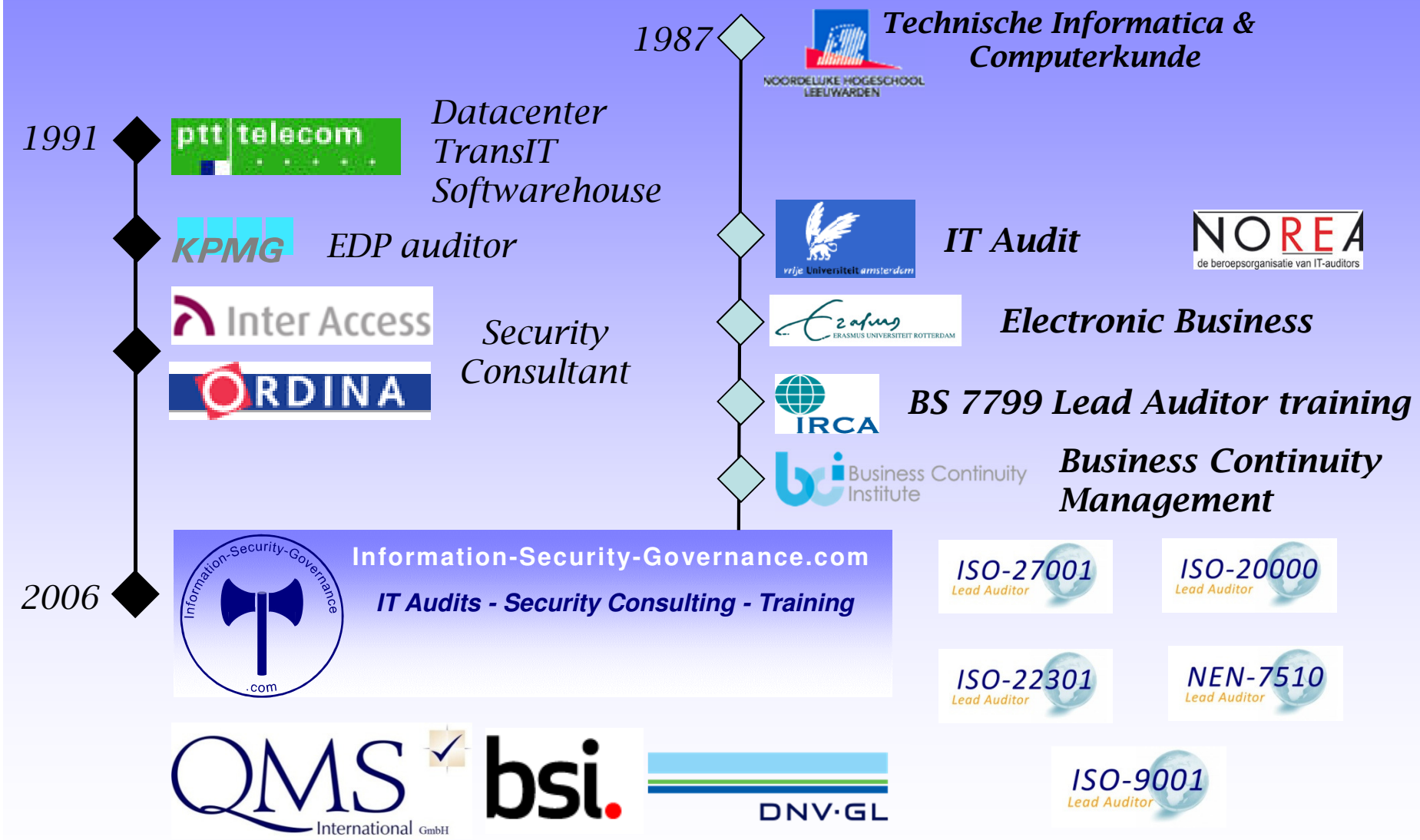
Haarlem, 18 maart 2014

Kwaliteitskring Noord-Holland

Agenda

- 13:45-14:15 - Informatiebeveiliging
  - Introductie
  - Informatiebeveiliging en ISO/IEC 27001
  - De nieuwste versie (2013) van 27001
  - Certificeren tegen ISO 27001
- 14:15-14:45 - Workshop ISMS
- 14:45-15:15 - Pauze
- 15:15-15:45 - Resultaten workshop

Introductie



Informatie

- Informatie is een belangrijk **bedrijfsmiddel**, dat net als andere belangrijke bedrijfsmiddelen, **onmisbaar** is voor de bedrijfsvoering en daardoor adequaat **beveiligd** moet worden (ISO 27000)

Doel van Informatiebeveiliging

Het garanderen van de

- **vertrouwelijkheid**
  - niet toegankelijk voor onbevoegden
- **integriteit**
  - juist en volledig
- **beschikbaarheid**
  - toegankelijk en bruikbaar

van informatie.

Managementsysteem voor Informatiebeveiliging

- Dat deel van een management-systeem dat op basis van een beoordeling van bedrijfsrisico's, tot doel heeft het vaststellen, implementeren, uitvoeren, controleren, beoordelen, onderhouden en verbeteren van informatiebeveiliging.

- Opmerking: Het managementsysteem omvat structuur, beleid, planningsactiviteiten, verantwoordelijkheden, werkwijzen, procedures, processen en middelen van de organisatie

ISO/IEC 27001

1980	**Shell Infosec Manual**	
1989	DTI CCSC Code of Practice	
1993	BSI DISC PD003 DTI Code of Practice	
1995	BS 7799-1	
1998		BS 7799-2
1999	BS 7799-1 revised	BS 7799-2 revised
2000	ISO 17799	
2002		BS 7799-2:2002
2004	*NEN 7510:2004*	
2005	ISO/IEC 17799	ISO/IEC 27001:2005
2007	ISO/IEC 27002	
2011		*NEN 7510*
2013	**ISO/IEC 27002**	**ISO/IEC 27001:2013**

Welkom bij de ISO 27000 familie

ISO/IEC 27000:2014	Information security management systems -- Overview and vocabulary
ISO/IEC 27001:2013	Information security management systems -- Requirements
ISO/IEC 27002:2013	Code of practice for information security controls
ISO/IEC 27003:2010	Information security management system implementation guidance
ISO/IEC 27004:2009	Information security management -- Measurement
ISO/IEC 27005:2011	Information security risk management
ISO/IEC 27006:2011	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007:2011	Guidelines for information security management systems auditing
ISO/IEC 27008:2011	Guidelines for auditors on information security controls
ISO/IEC 27009	The Use and Application of ISO/IEC 27001 for Sector/Service-Specific Third-Party Accredited Certifications
ISO/IEC 27010:2012	Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011:2008	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27013:2012	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27014:2013	Governance of information security
ISO/IEC 27015:2012	Information security management guidelines for financial services
ISO/IEC 27016:2014	Information security management -- Organizational economics
ISO/IEC 27017	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002
ISO/IEC 27018	Code of practice for PII protection in public cloud acting as PII processors
ISO/IEC 27019:2013	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

ISO Werk in uitvoering

ISO/IEC 27031:2011	Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032:2012	Guidelines for cybersecurity
ISO/IEC 27033	Network security
ISO/IEC 27034	Application security
ISO/IEC 27035:2011	Information security incident management
ISO/IEC 27036	Information security for supplier relationships
ISO/IEC 27037:2012	Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038:2014	Specification for digital redaction
ISO/IEC 27039	Selection, deployment and operations of intrusion detection systems (IDPS)
ISO/IEC 27040	Storage security
ISO/IEC 27041	Guidance on assuring suitability and adequacy of incident investigative methods
ISO/IEC 27042	Guidelines for the analysis and interpretation of digital evidence
ISO/IEC 27043	Incident investigation principles and processes
ISO/IEC 27044	Guidelines for Security Information and Event Management (SIEM)
ISO/IEC 27050	Electronic discovery

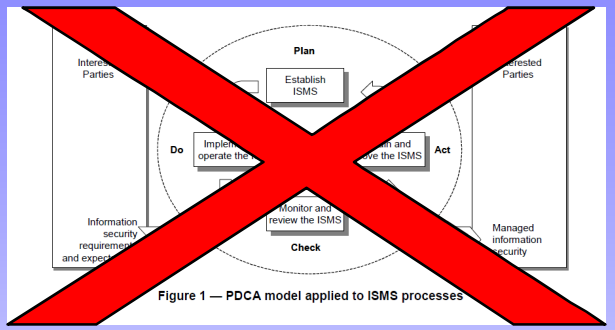
ISO 27001 wijzigingen (2013)

- De “oude” standaard is vervangen.
- Gestandaardiseerde structuur:
  - de structuur en inhoud van de tekst is veranderd
  - Appendix 3 van ISO/IEC Directives, Part 1 **Annex SL**

Annex SL

Introduction

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organisation
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement



High level structure (27001)

- 4 Context of the organization
  - 4.1 Understanding the organization and its context
  - 4.2 Understanding the needs and expectations of interested parties
  - 4.3 Determining the scope of the **IS** management system
  - 4.4 **IS** management system
- 5 Leadership
  - 5.1 Leadership and commitment
  - 5.2 Policy
  - 5.3 Organizational roles, responsibilities and authorities
- 6 Planning
  - 6.1 Actions to address risks and opportunities
  - 6.2 **IS** objectives and planning to achieve them
- 7 Support
  - 7.1 Resources
  - 7.2 Competence
  - 7.3 Awareness
  - 7.4 Communication
  - 7.5 Documented information
- 8 Operation
  - 8.1 Operational planning and control
  - *8.2 Information security risk assessment*
  - *8.3 Information security risk treatment*
- 9 Performance evaluation
  - 9.1 Monitoring, measurement, analysis and evaluation
  - 9.2 Internal audit
  - 9.3 Management review
- 10 Improvement
  - 10.1 Nonconformity and corrective action
  - 10.2 Continual improvement

High level structure (9001)

4 Context of the organization

- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the **IS** management system
- 4.4 **IS** management system

5 Leadership

- 5.1 Leadership and commitment
- 5.2 Policy
- 5.3 Organizational roles, responsibilities and authorities

6 Planning

- 6.1 Actions to address risks and opportunities
- 6.2 **IS** objectives and planning to achieve them
- ~ *Planning of changes*

7 Support

- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information

8 Operation

- 8.1 Operational planning and control
- ~ *Determination of market needs and interaction with customers*
- ~ *Operational planning process*
- ~ *Control of external provisions of goods and services*
- ~ *Development of goods and services*
- ~ *Production of goods and provision of services*
- ~ *Release of goods and services*
- ~ *Non conforming goods and services*

10 Improvement

- 10.1 Nonconformity and corrective action
- 10.2 Continual improvement

Documented Information

- “De organisatie dient gedocumenteerde informatie zodanig bij te houden dat er voldoende vertrouwen is dat de processen zijn uitgevoerd zoals gepland. "

- Scope
- Informatiebeveiligingsbeleid
- Statement of Applicability (Verklaring van Toepasselijkheid)
- Gedocumenteerde informatie over:
  - het risico analyse proces.
  - risico management proces
  - doelstellingen op het gebeid van informatiebeveiliging.
- Resultaten van:
  - de risico analyses.
  - resultaten van risico management.
  - correctieve maatregelen.
- Bewijs van:
  - competenties.
  - bewaking en metingen.
  - het audit programma en audit resultaten.
  - directiebeoordelingen.
  - de aard van afwijkingen en genomen acties

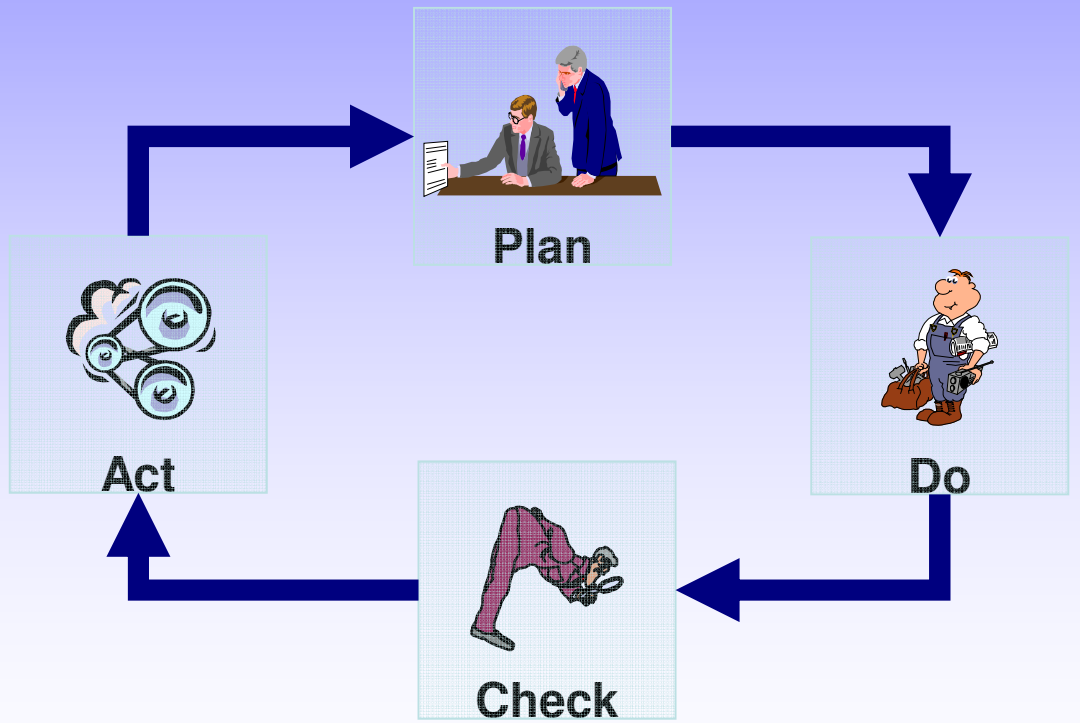
ISO 27001 Annex A (normative)

Reference control objectives and controls

- A.5 Security policies
- A.6 Organisation of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 Systems acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Incident management
- A.17 Business continuity management
- A.18 Compliance

IS management systeem

4. Context of the organisation
5. Leadership
6. Planning
7. Support

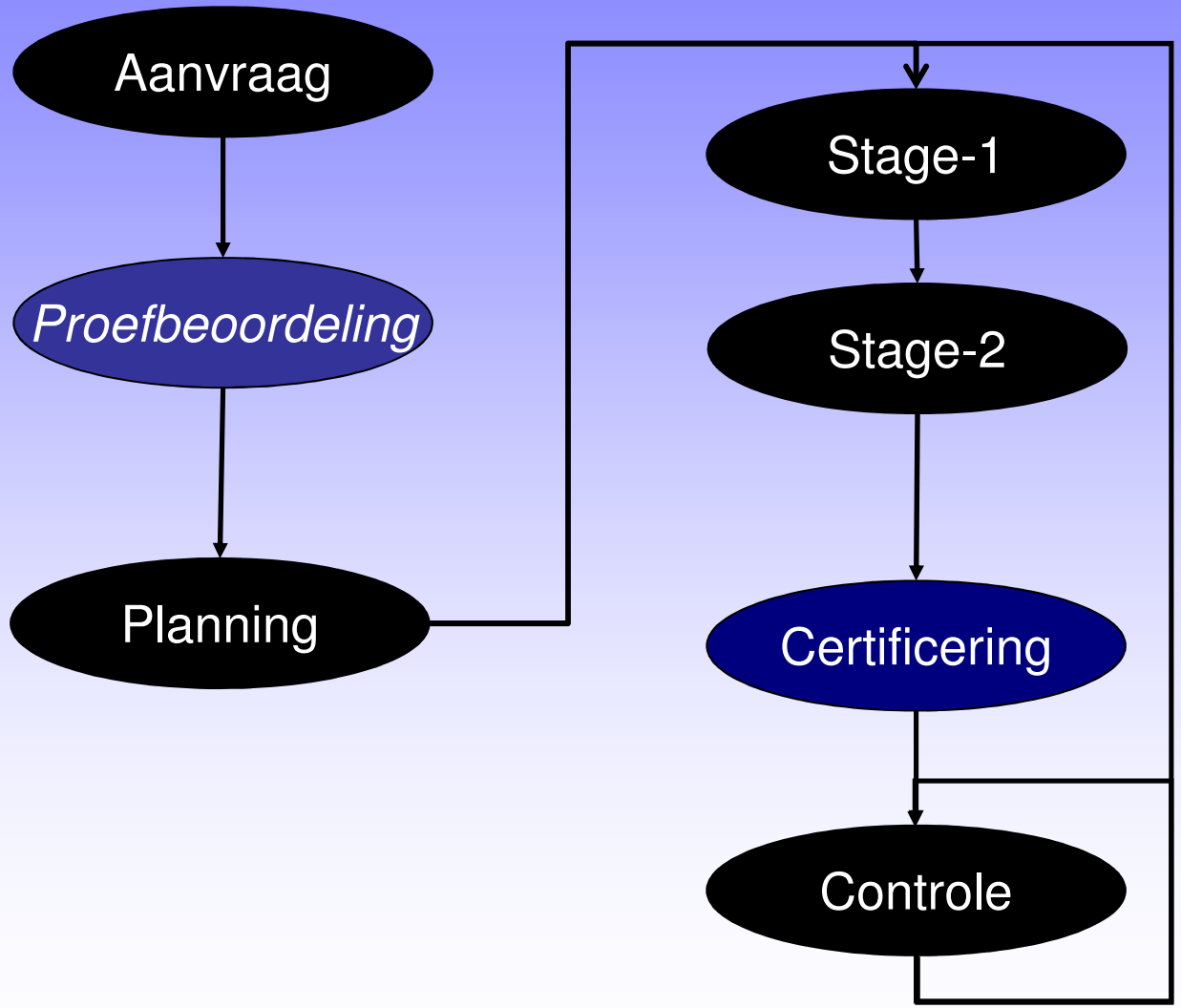


10. Improvement

8. Operation
- *IS risk assessment*
- *IS risk treatment*

9. Performance evaluation

Certificering



De praktijk case

Praktijk case

- Wij zijn als bierbrouwerij gevraagd om onze producten te leveren aan het Holland House tijdens het WK 2014.
- Men wil met ons een langlopend contract aangaan voor levering tijdens alle komende EK's en WK's.
- Voorwaarde: wij moeten kunnen aantonen dat onze informatie-voorziening betrouwbaar is

Onze bierbrouwerij

- Waarom is betrouwbare informatie-voorziening zo belangrijk?
  - Ons imago voor het Holland Huis.
  - Te allen tijde kunnen leveren om kostenneutraal te kunnen zijn.
  - De vertrouwelijkheid van (het drinkgedrag van) de gasten en VIP's!
  - Cijfers over "verbruik" van ons bier is essentiële input voor het logistieke proces!
  - …

We willen een ISMS!

- **Hoe gaan we zorgen dat we de betrouwbaarheid van onze informatie kunnen garanderen?**

- *Hint: laten we een **management systeem** voor Informatiebeveiliging inrichten (conform ISO 27001)*

Opdracht

- Welke stappen zijn nodig om een ISMS in te richten.
- Denk daarbij aan ieder ander management systeem dat u kent.

High level structure

- 4 Context of the organization
  - 4.1 Understanding the organization and its context
  - 4.2 Understanding the needs and expectations of interested parties
  - 4.3 Determining the scope of the **IS** management system
  - 4.4 **IS** management system
- 5 Leadership
  - 5.1 Leadership and commitment
  - 5.2 Policy
  - 5.3 Organizational roles, responsibilities and authorities
- 6 Planning
  - 6.1 Actions to address risks and opportunities
  - 6.2 **IS** objectives and planning to achieve them
- 7 Support
  - 7.1 Resources
  - 7.2 Competence
  - 7.3 Awareness
  - 7.4 Communication
  - 7.5 Documented information
- 8 Operation
  - 8.1 Operational planning and control
  - *8.2 Information security risk assessment*
  - *8.3 Information security risk treatment*
- 9 Performance evaluation
  - 9.1 Monitoring, measurement, analysis and evaluation
  - 9.2 Internal audit
  - 9.3 Management review
- 10 Improvement
  - 10.1 Nonconformity and corrective action
  - 10.2 Continual improvement

De resultaten van de workshop

Bedankt voor uw aandacht!

Vragen

Opmerkingen

Suggesties

Aart.Bitter@isgcom.nl