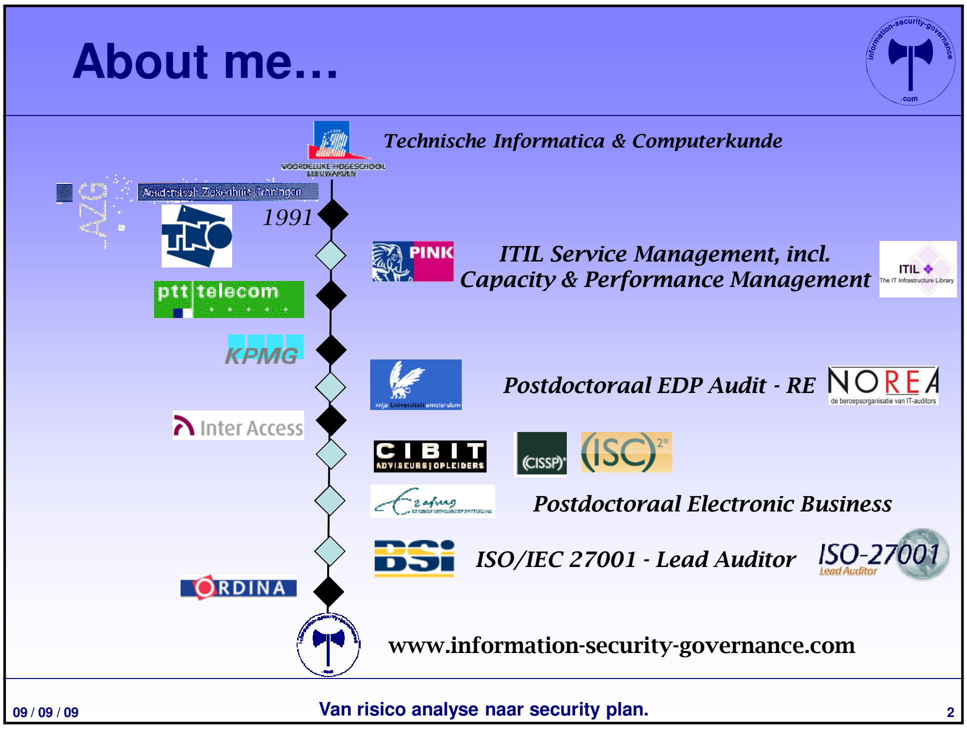
Van risico analyse naar security plan.

Small step (for man)
or
Giant leap (for mankind)

Aart Bitter
9 september 2009

Aart.Bitter@planet.nl



About me…

Technische Informatica & Computerkunde

1991

ITIL Service Management, incl. Capacity & Performance Management

Postdoctoraal EDP Audit - RE

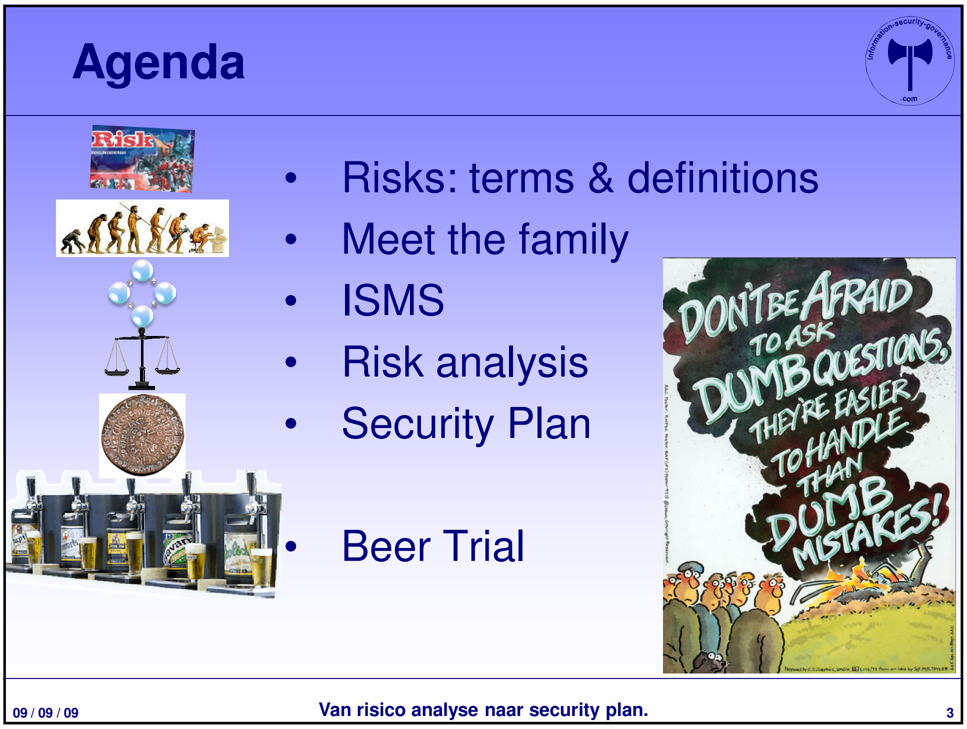
Postdoctoraal Electronic Business

ISO/IEC 27001 - Lead Auditor

www.information-security-governance.com

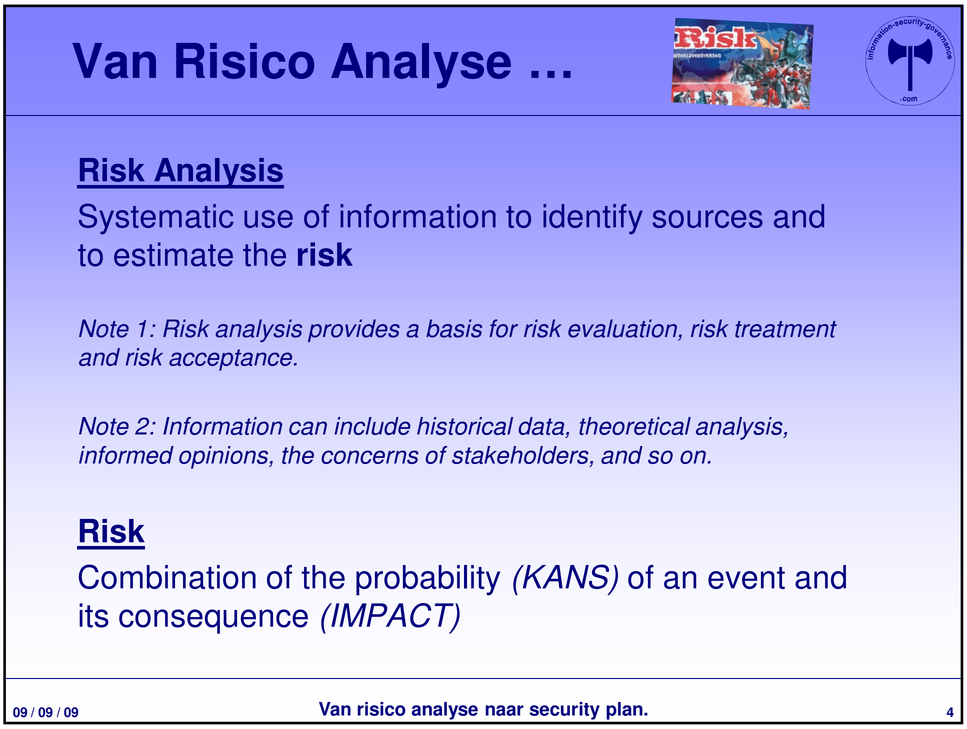
Noordelijke Hogeschool Leeuwarden
AZG
Academisch Ziekenhuis Groningen
TNO
ptt telecom
KPMG
Inter Access
ORDINA
PINK
ITIL The IT Infrastructure Library
vrije Universiteit amsterdam
NOREA de beroepsorganisatie van IT-auditors
CIBIT ADVISEURS | OPLEIDERS
CISSP
(ISC)²
Erasmus
BSi
ISO-27001 Lead Auditor

09 / 09 / 09 Van risico analyse naar security plan. 2


Risk
DON'T BE AFRAID TO ASK DUMB QUESTIONS, THEY'RE EASIER TO HANDLE THAN DUMB MISTAKES!

Agenda

- Risks: terms & definitions
- Meet the family
- ISMS
- Risk analysis
- Security Plan
- Beer Trial



Van Risico Analyse …

Risk Analysis

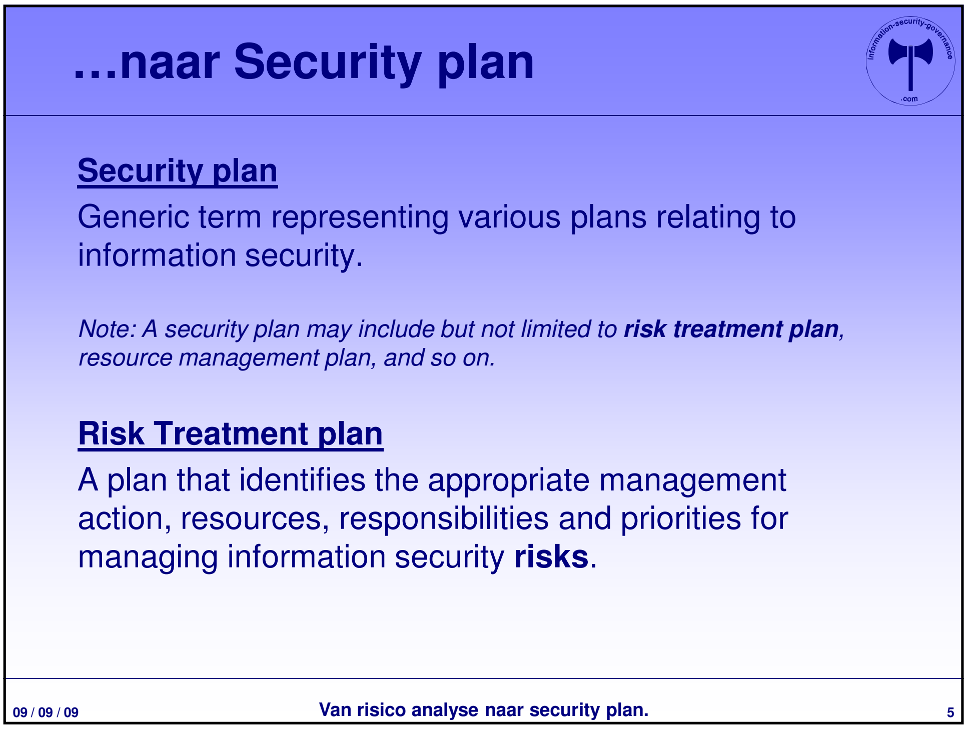
Systematic use of information to identify sources and to estimate the **risk**

Note 1: Risk analysis provides a basis for risk evaluation, risk treatment and risk acceptance.

Note 2: Information can include historical data, theoretical analysis, informed opinions, the concerns of stakeholders, and so on.

Risk

Combination of the probability *(KANS)* of an event and its consequence *(IMPACT)*



…naar Security plan

Security plan

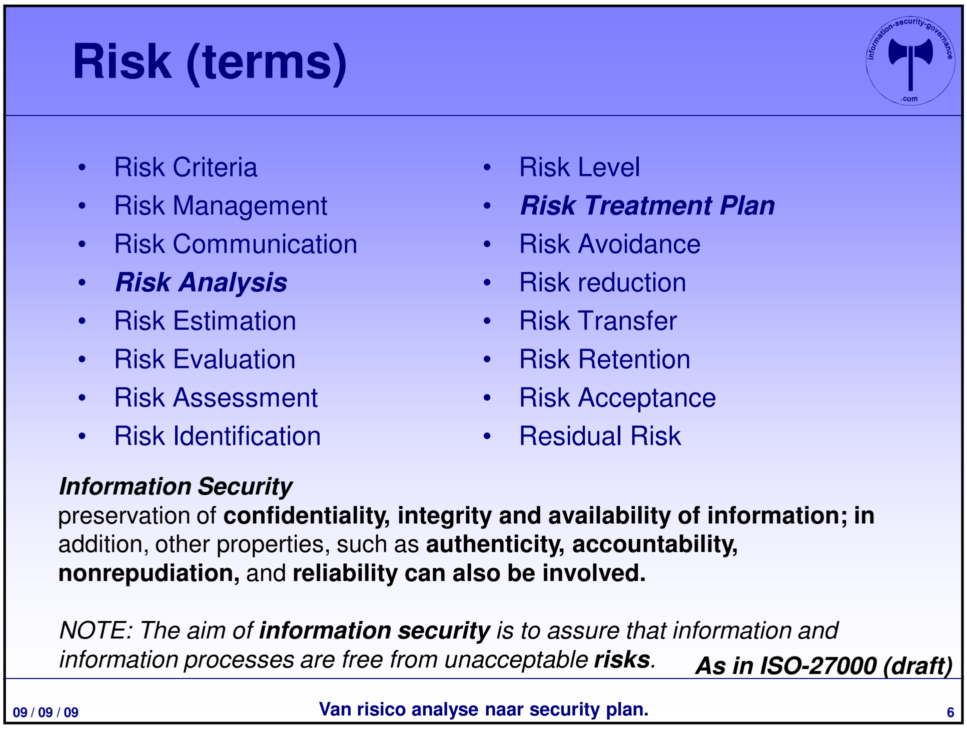
Generic term representing various plans relating to information security.

*Note: A security plan may include but not limited to **risk treatment plan**, resource management plan, and so on.*

Risk Treatment plan

A plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security **risks**.

09 / 09 / 09 Van risico analyse naar security plan. 5



Risk (terms)

- Risk Criteria
- Risk Management
- Risk Communication
- ***Risk Analysis***
- Risk Estimation
- Risk Evaluation
- Risk Assessment
- Risk Identification
- Risk Level
- ***Risk Treatment Plan***
- Risk Avoidance
- Risk reduction
- Risk Transfer
- Risk Retention
- Risk Acceptance
- Residual Risk

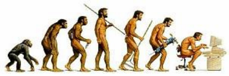
Information Security
preservation of **confidentiality, integrity and availability of information; in** addition, other properties, such as **authenticity, accountability, nonrepudiation,** and **reliability can also be involved.**

*NOTE: The aim of **information security** is to assure that information and information processes are free from unacceptable **risks**.*

As in ISO-27000 (draft)

09 / 09 / 09 Van risico analyse naar security plan. 6

Meet the family …

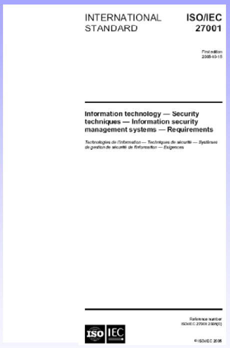


ISO/IEC 27000	Fundamentals and vocabulary
ISO/IEC 27001	Information Security Management Systems Requirements
ISO/IEC 27002	Code of Practice for information security management (**ISO-17799**)
ISO/IEC 27003	Implementation Guidance
ISO/IEC 27004	Information security management measurements
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for certification bodies
ISO/IEC 27007	Guidelines for Information security management systems auditing
ISO/IEC 27011	Information security management guidelines for telecommunications
ISO/IEC 27031	Business Continuity
ISO/IEC 27032	Guidelines for cybersecurity
ISO/IEC 27033	IT network security
ISO/IEC 27034	Guidelines for application security
ISO/IEC 27799	Security Management in Health
Up to ISO 27059	Reserved for future standards

ISO/IEC 27001 & ISO/IEC 27002

ISO/IEC 27001

Requirements for "Information Security Management Systems"



INTERNATIONAL STANDARD ISO/IEC 27001

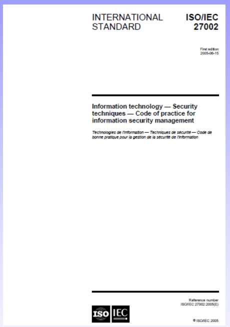
First edition 2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Reference number ISO/IEC 27001:2005(E)

© ISO/IEC 2005



INTERNATIONAL STANDARD ISO/IEC 27002

First edition 2005-06-15

Information technology — Security techniques — Code of practice for information security management

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information

Reference number ISO/IEC 27002:2005(E)

© ISO/IEC 2005

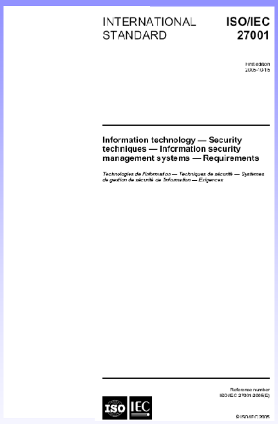
ISO/IEC 27002

Code of Practice for Information Security Management

Evolution of Standards

1993	Code of practice	
1995	British Standard BS 7799-1	
1998		BS 7799-2
1999	BS 7799-1 revised	BS 7799-2 revised
2000	ISO 17799	
2002		BS 7799-2:2002
2005	ISO/IEC 17799:2005	
2005/11		**ISO/IEC 27001**
2007/07	**ISO/IEC 27002**	

ORGANISATION INTERNATIONALE DE NORMALISATION ISO INTERNATIONAL ORGANIZATION FOR STANDARDIZATION



INTERNATIONAL STANDARD ISO/IEC 27001

First edition 2005-10-15

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Reference number ISO/IEC 27001:2005(E)

© ISO/IEC 2005

INTERNATIONAL STANDARD ISO/IEC 27002

First edition 2005-06-15

Information technology — Security techniques — Code of practice for information security management

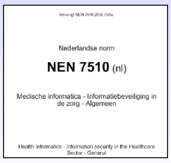
Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information

Reference number ISO/IEC 27002:2005(E)

© ISO/IEC 2005

NEN

Code voor informatiebeveiliging



Vervangt NEN 7510:2002 Ontw.

Nederlandse norm

NEN 7510 (nl)

Medische informatica - Informatiebeveiliging in de zorg - Algemeen

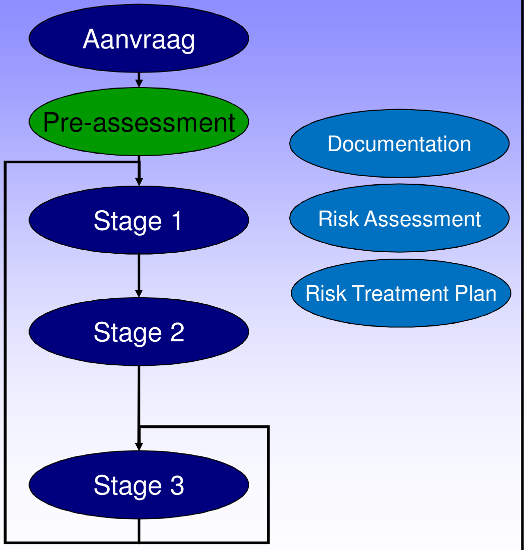
Health informatics - Information security in the Healthcare Sector - General

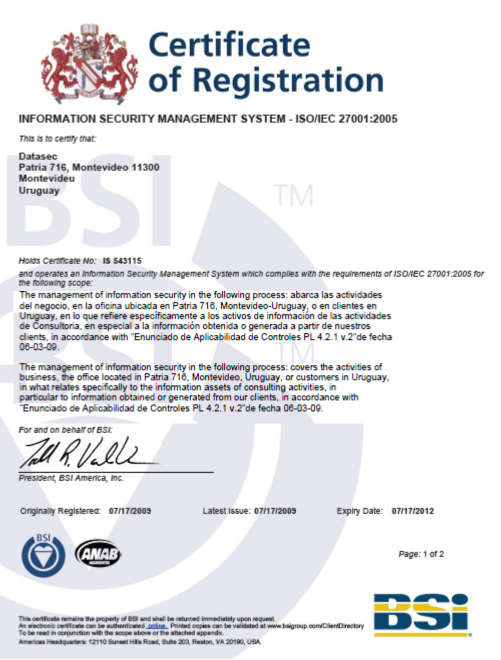
ISO-27001 certificering

“desktop review“ of the existence and completeness of key documentation such as the organization's security policy, Statement of Applicability (SoA) and Risk Treatment Plan (RTP).

in-depth audit involving testing the existence and effectiveness of the ISMS and information security controls stated in the SoA and RTP, as well as their supporting documentation.

is a reassessment audit to confirm that a previously-certified organization remains in compliance with the standard.





Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2005

This is to certify that:

Datasec
Patria 716, Montevideo 11300
Montevideu
Uruguay

Holds Certificate No: **IS 543115**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2005 for the following scope:

The management of information security in the following process: abarca las actividades del negocio, en la oficina ubicada en Patria 716, Montevideo-Uruguay, o en clientes en Uruguay, en lo que refiere específicamente a los activos de información de las actividades de Consultoria, en especial a la información obtenida o generada a partir de nuestros clients, in accordance with "Enunciado de Aplicabilidad de Controles PL 4.2.1 v.2"de fecha 06-03-09.

The management of information security in the following process: covers the activities of business, the office located in Patria 716, Montevideo, Uruguay, or customers in Uruguay, in what relates specifically to the information assets of consulting activities, in particular to information obtained or generated from our clients, in accordance with "Enunciado de Aplicabilidad de Controles PL 4.2.1 v.2"de fecha 06-03-09.

For and on behalf of BSI:

President, BSI America, Inc.

Originally Registered: **07/17/2009** Latest Issue: **07/17/2009** Expiry Date: **07/17/2012**

Page: 1 of 2

This certificate remains the property of BSI and shall be returned immediately upon request.
An electronic certificate can be authenticated online. Printed copies can be validated at www.bsigroup.com/ClientDirectory
To be read in conjunction with the scope above or the attached appendix.
Americas Headquarters: 12110 Sunset Hills Road, Suite 200, Reston, VA 20190, USA.

ISMS Definition

An

***I**nformation **S**ecurity **M**anagement **S**ystem*

is the part of the overall management system that,

based on a **business risk approach**,

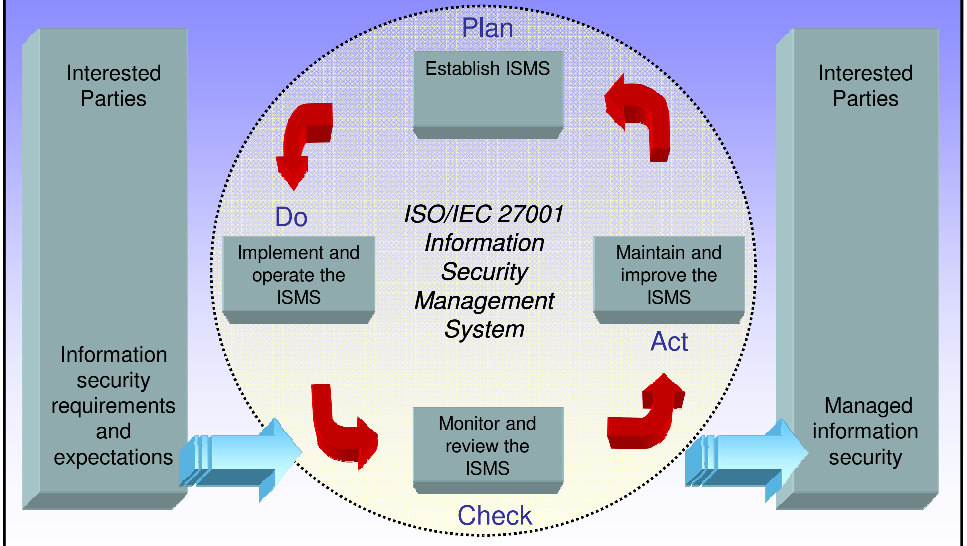
is intended to **ensure** the

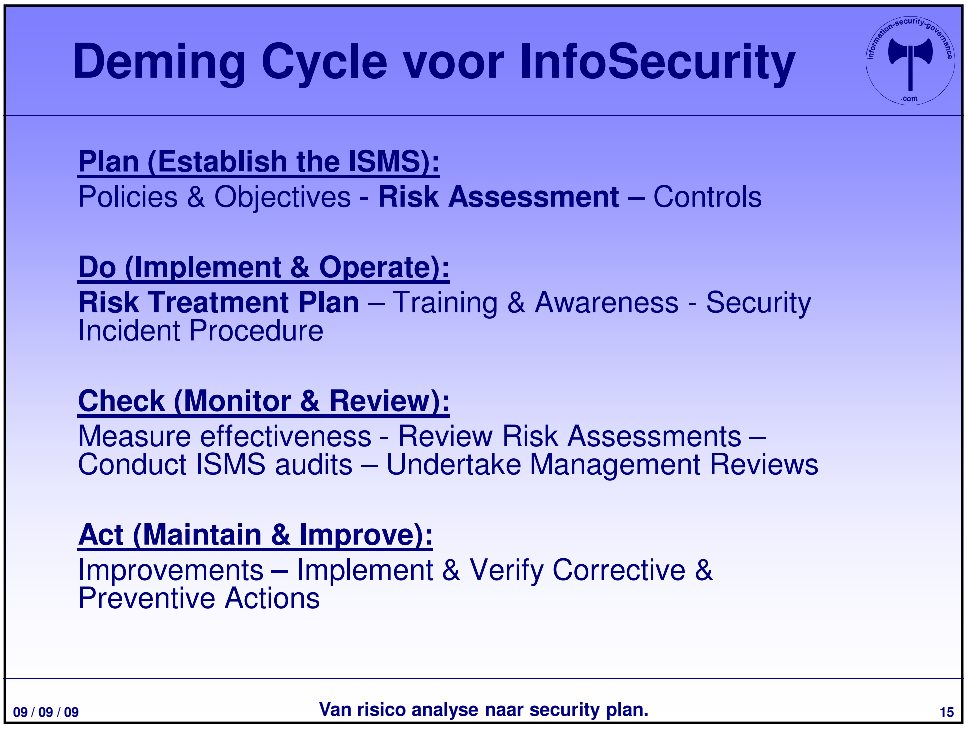
availability, **confidentiality** & **integrity**

of information and associated assets.

Management system: a system to establish and achieve policy and objectives.
System: a set of interrelated or interacting elements.

The Quest


Interested Parties
Information security requirements and expectations
Plan
Establish ISMS
Do
Implement and operate the ISMS
ISO/IEC 27001 Information Security Management System
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested Parties
Managed information security



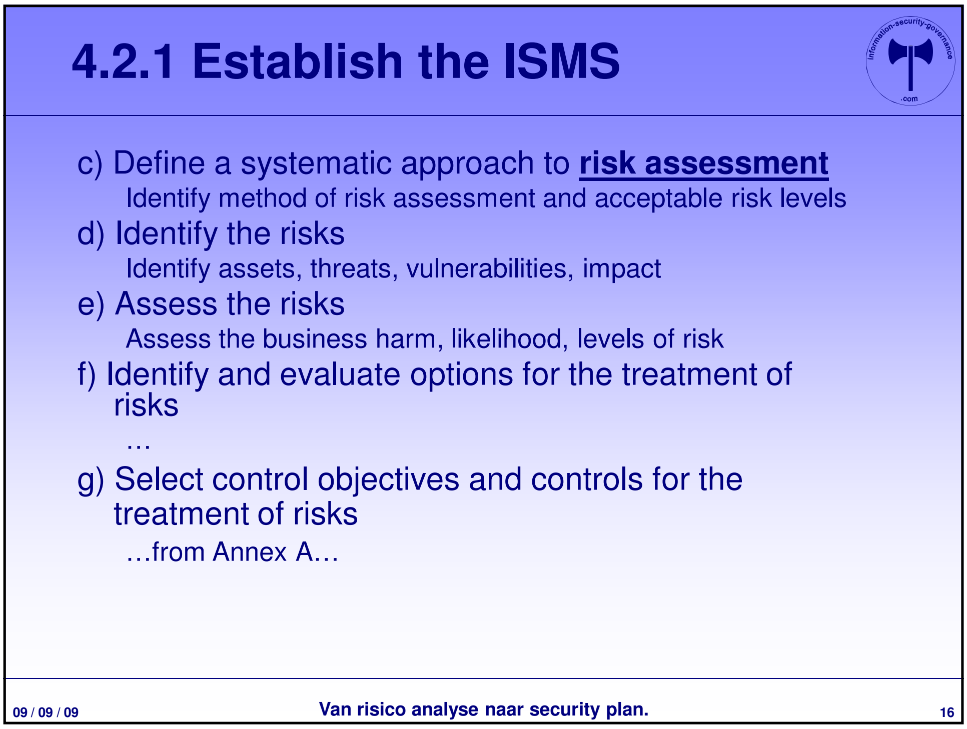
Deming Cycle voor InfoSecurity

Plan (Establish the ISMS):
Policies & Objectives - **Risk Assessment** – Controls

Do (Implement & Operate):
Risk Treatment Plan – Training & Awareness - Security Incident Procedure

Check (Monitor & Review):
Measure effectiveness - Review Risk Assessments – Conduct ISMS audits – Undertake Management Reviews

Act (Maintain & Improve):
Improvements – Implement & Verify Corrective & Preventive Actions



4.2.1 Establish the ISMS

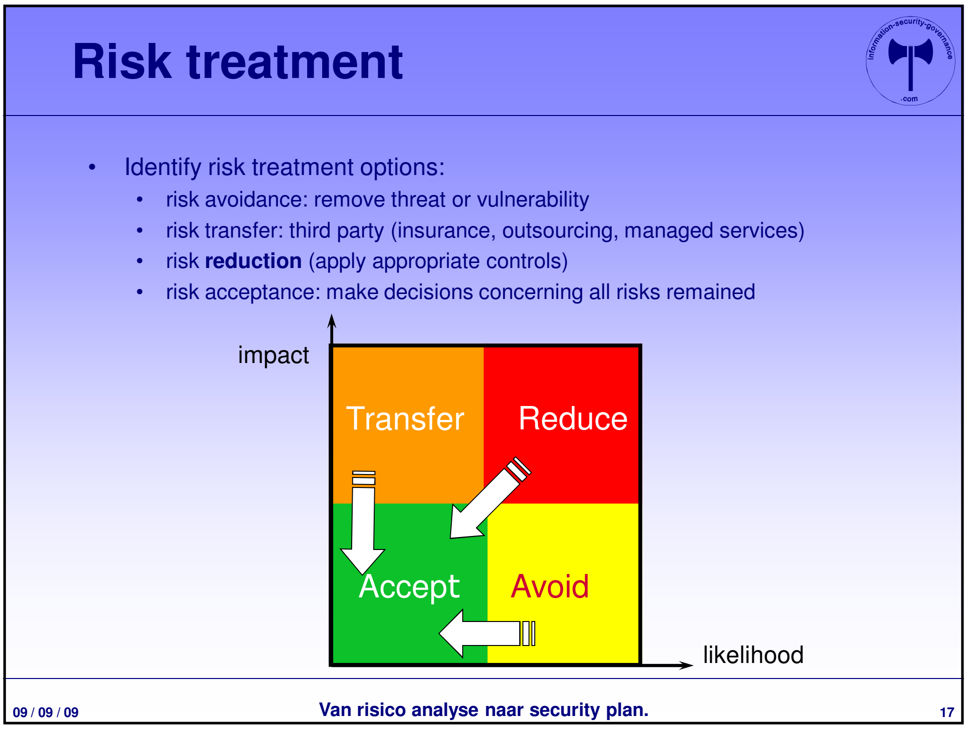
c) Define a systematic approach to **risk assessment**
  Identify method of risk assessment and acceptable risk levels

d) Identify the risks
  Identify assets, threats, vulnerabilities, impact

e) Assess the risks
  Assess the business harm, likelihood, levels of risk

f) Identify and evaluate options for the treatment of risks
  …

g) Select control objectives and controls for the treatment of risks
  …from Annex A…



Risk treatment

- Identify risk treatment options:
  - risk avoidance: remove threat or vulnerability
  - risk transfer: third party (insurance, outsourcing, managed services)
  - risk **reduction** (apply appropriate controls)
  - risk acceptance: make decisions concerning all risks remained

impact

Transfer

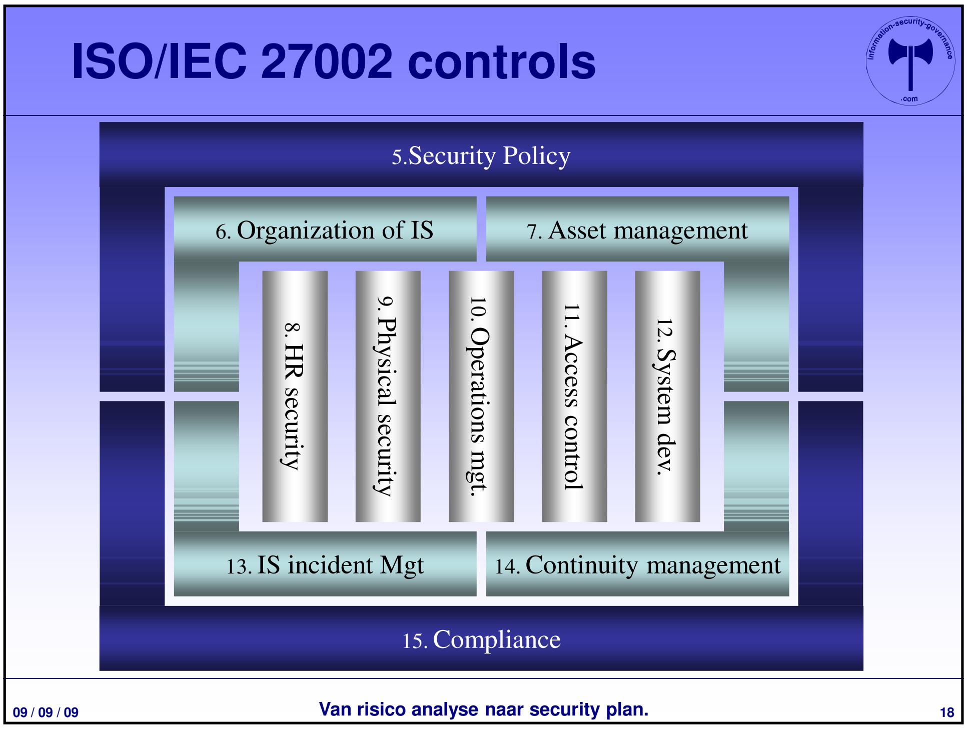
Reduce

Accept

Avoid

likelihood

09 / 09 / 09 Van risico analyse naar security plan. 17



ISO/IEC 27002 controls

5.Security Policy

6. Organization of IS

7. Asset management

8. HR security

9. Physical security

10. Operations mgt.

11. Access control

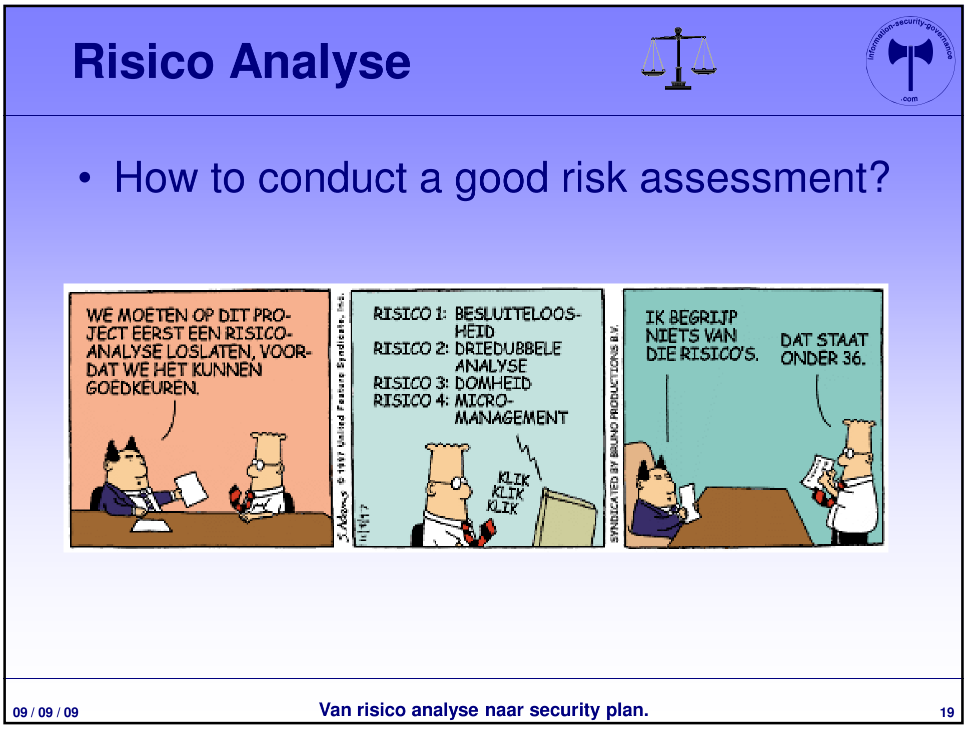
12. System dev.

13. IS incident Mgt

14. Continuity management

15. Compliance

09 / 09 / 09 Van risico analyse naar security plan. 18

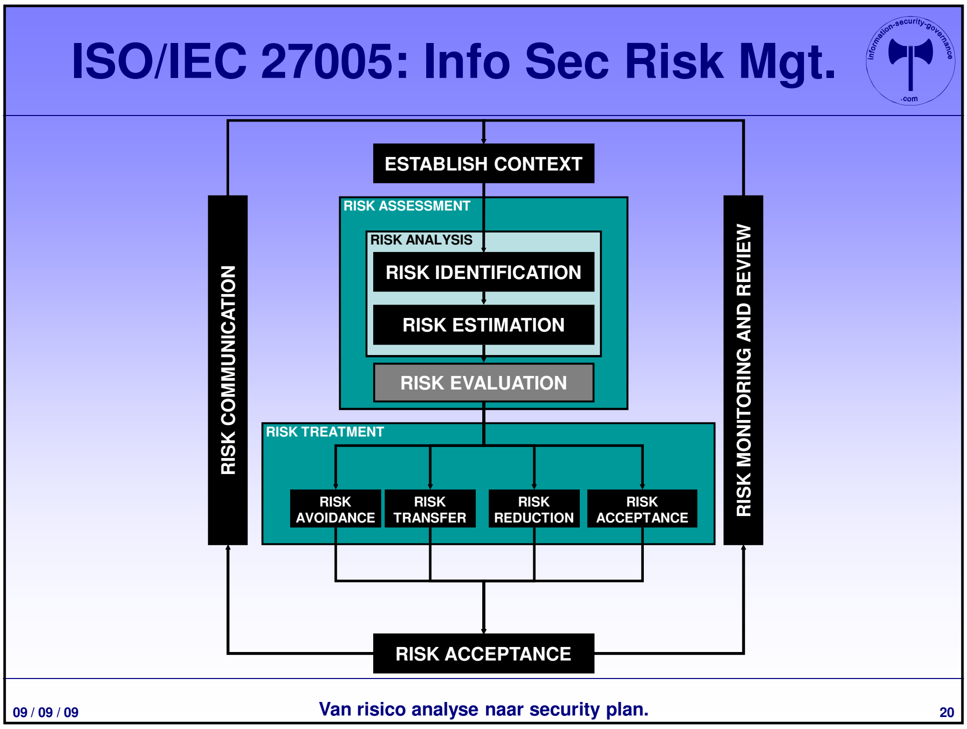


Risico Analyse

- How to conduct a good risk assessment?

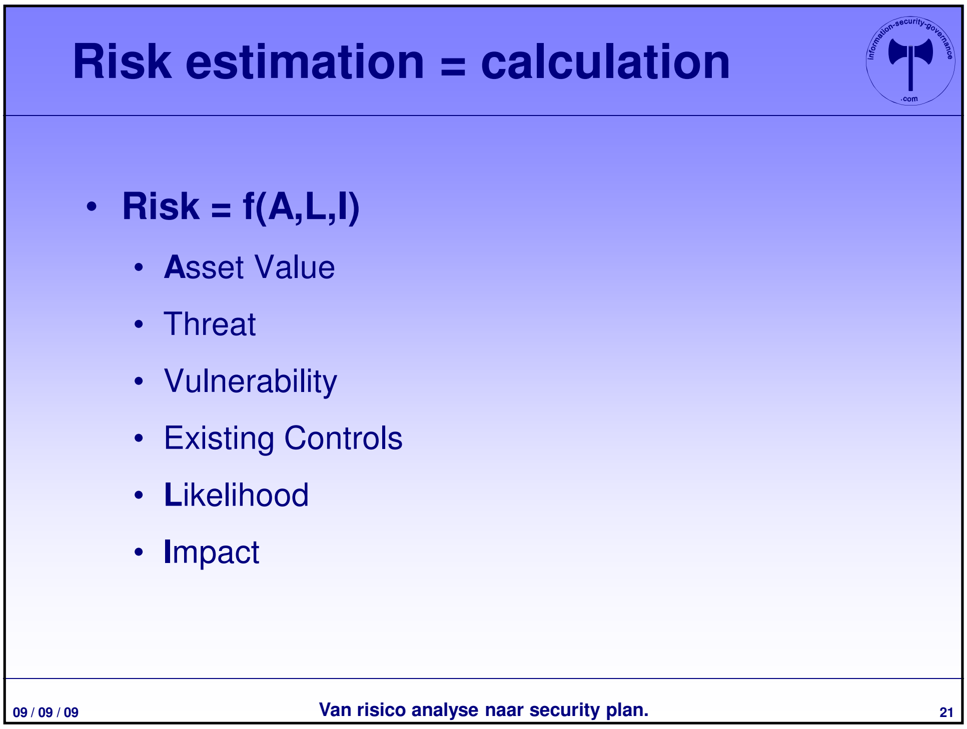
WE MOETEN OP DIT PROJECT EERST EEN RISICO-ANALYSE LOSLATEN, VOORDAT WE HET KUNNEN GOEDKEUREN.
RISICO 1: BESLUITELOOSHEID
RISICO 2: DRIEDUBBELE ANALYSE
RISICO 3: DOMHEID
RISICO 4: MICRO-MANAGEMENT
KLIK KLIK KLIK
IK BEGRIJP NIETS VAN DIE RISICO'S.
DAT STAAT ONDER 36.
© 1997 United Feature Syndicate, Inc.
SYNDICATED BY BRUNO PRODUCTIONS B.V.
S. Adams 11/9/97

09 / 09 / 09 Van risico analyse naar security plan. 19



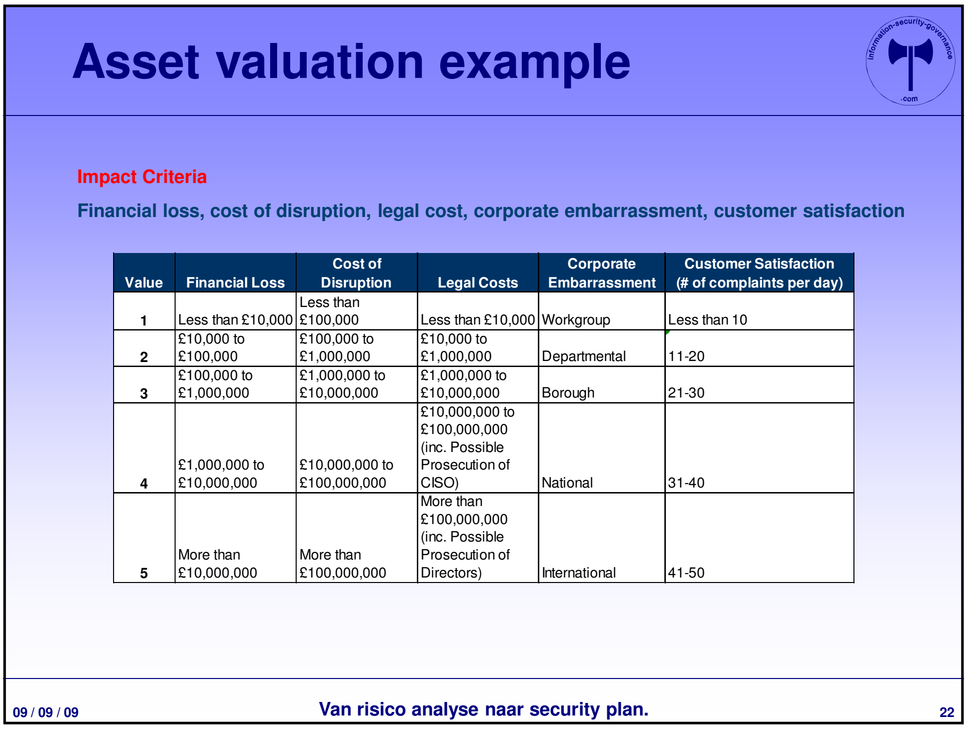
ISO/IEC 27005: Info Sec Risk Mgt.

09 / 09 / 09 Van risico analyse naar security plan. 20



Risk estimation = calculation

- **Risk = f(A,L,I)**
  - **A**sset Value
  - Threat
  - Vulnerability
  - Existing Controls
  - **L**ikelihood
  - **I**mpact

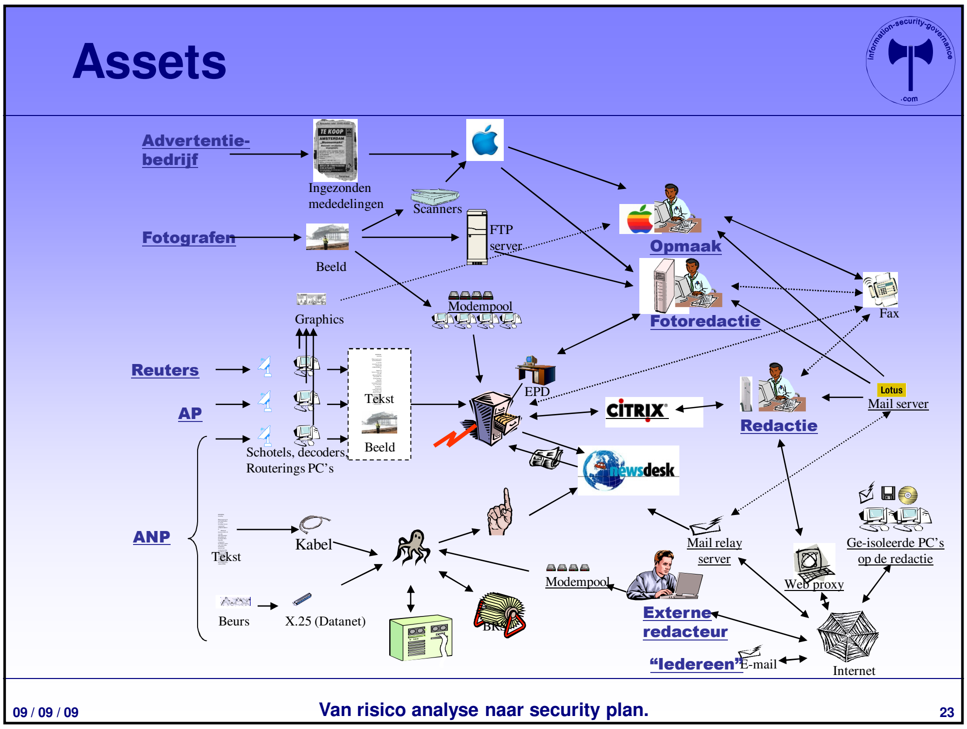


Asset valuation example

Impact Criteria

Financial loss, cost of disruption, legal cost, corporate embarrassment, customer satisfaction

Value	Financial Loss	Cost of Disruption	Legal Costs	Corporate Embarrassment	Customer Satisfaction (# of complaints per day)
1	Less than £10,000	Less than £100,000	Less than £10,000	Workgroup	Less than 10
2	£10,000 to £100,000	£100,000 to £1,000,000	£10,000 to £1,000,000	Departmental	11-20
3	£100,000 to £1,000,000	£1,000,000 to £10,000,000	£1,000,000 to £10,000,000	Borough	21-30
4	£1,000,000 to £10,000,000	£10,000,000 to £100,000,000	£10,000,000 to £100,000,000 (inc. Possible Prosecution of CISO)	National	31-40
5	More than £10,000,000	More than £100,000,000	More than £100,000,000 (inc. Possible Prosecution of Directors)	International	41-50



Assets

Advertentie-bedrijf

Ingezonden mededelingen

Scanners

Fotografen

Beeld

FTP server

Graphics

Modempool

Opmaak

Fotoredactie

Fax

Reuters

AP

Tekst

Beeld

Schotels, decoders, Routerings PC's

EPD

CITRIX

Redactie

Lotus Mail server

newsdesk

ANP

Tekst

Kabel

Beurs

X.25 (Datanet)

BKS

Modempool

Mail relay server

Web proxy

Ge-isoleerde PC's op de redactie

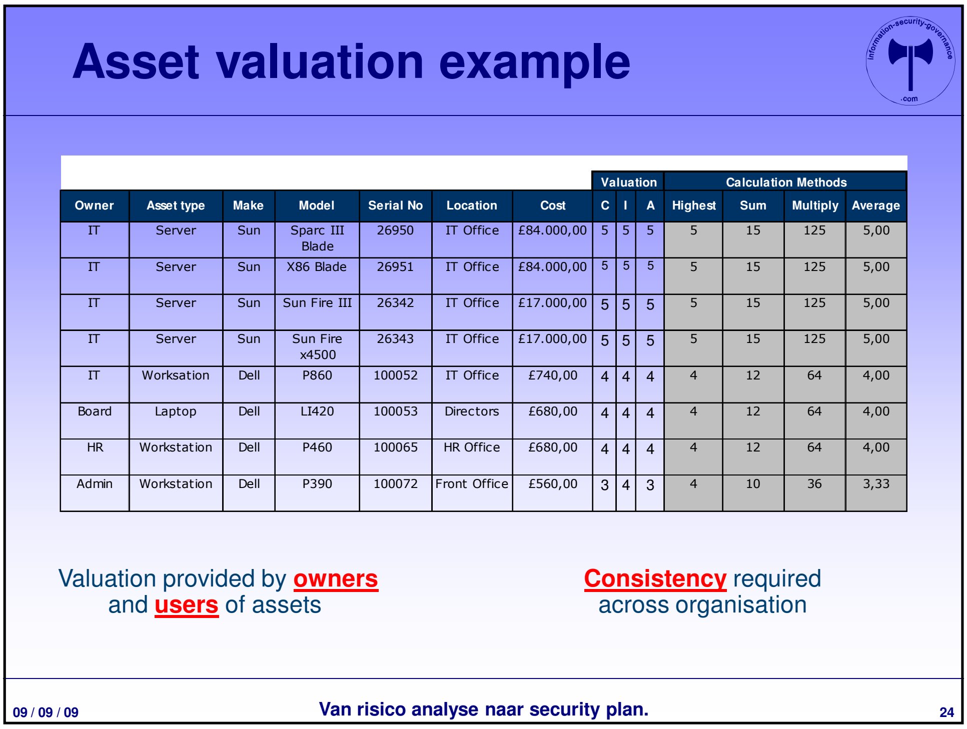
Externe redacteur

"Iedereen"

E-mail

Internet

09 / 09 / 09 Van risico analyse naar security plan. 23



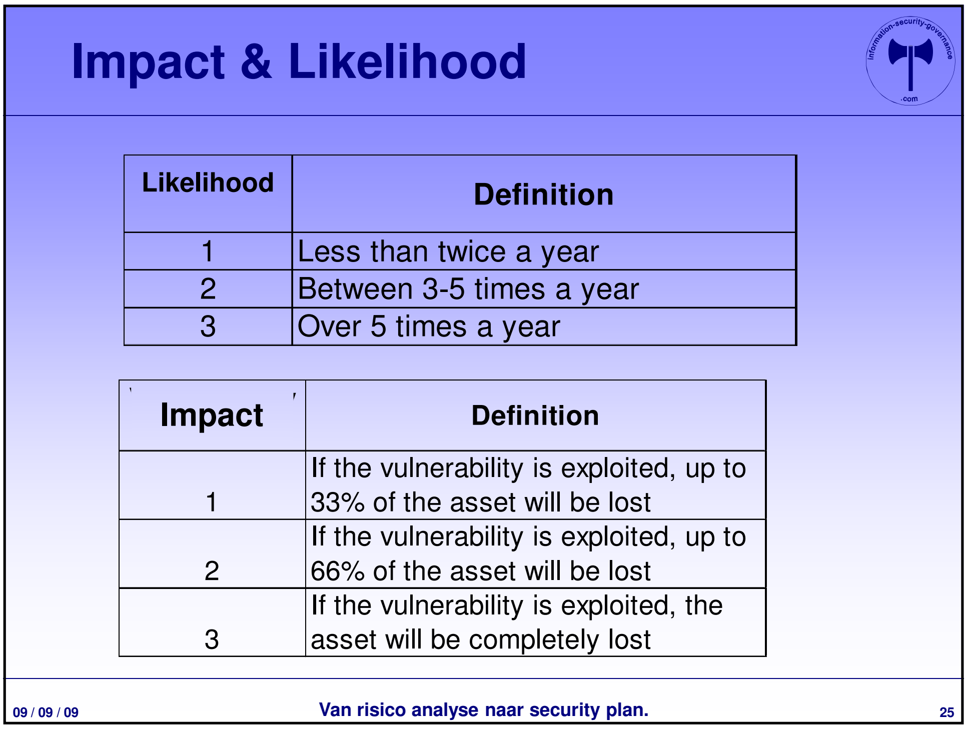
Asset valuation example

							Valuation			Calculation Methods			
Owner	Asset type	Make	Model	Serial No	Location	Cost	C	I	A	Highest	Sum	Multiply	Average
IT	Server	Sun	Sparc III Blade	26950	IT Office	£84.000,00	5	5	5	5	15	125	5,00
IT	Server	Sun	X86 Blade	26951	IT Office	£84.000,00	5	5	5	5	15	125	5,00
IT	Server	Sun	Sun Fire III	26342	IT Office	£17.000,00	5	5	5	5	15	125	5,00
IT	Server	Sun	Sun Fire x4500	26343	IT Office	£17.000,00	5	5	5	5	15	125	5,00
IT	Worksation	Dell	P860	100052	IT Office	£740,00	4	4	4	4	12	64	4,00
Board	Laptop	Dell	LI420	100053	Directors	£680,00	4	4	4	4	12	64	4,00
HR	Workstation	Dell	P460	100065	HR Office	£680,00	4	4	4	4	12	64	4,00
Admin	Workstation	Dell	P390	100072	Front Office	£560,00	3	4	3	4	10	36	3,33

Valuation provided by **owners** and **users** of assets

Consistency required across organisation

09 / 09 / 09 Van risico analyse naar security plan. 24

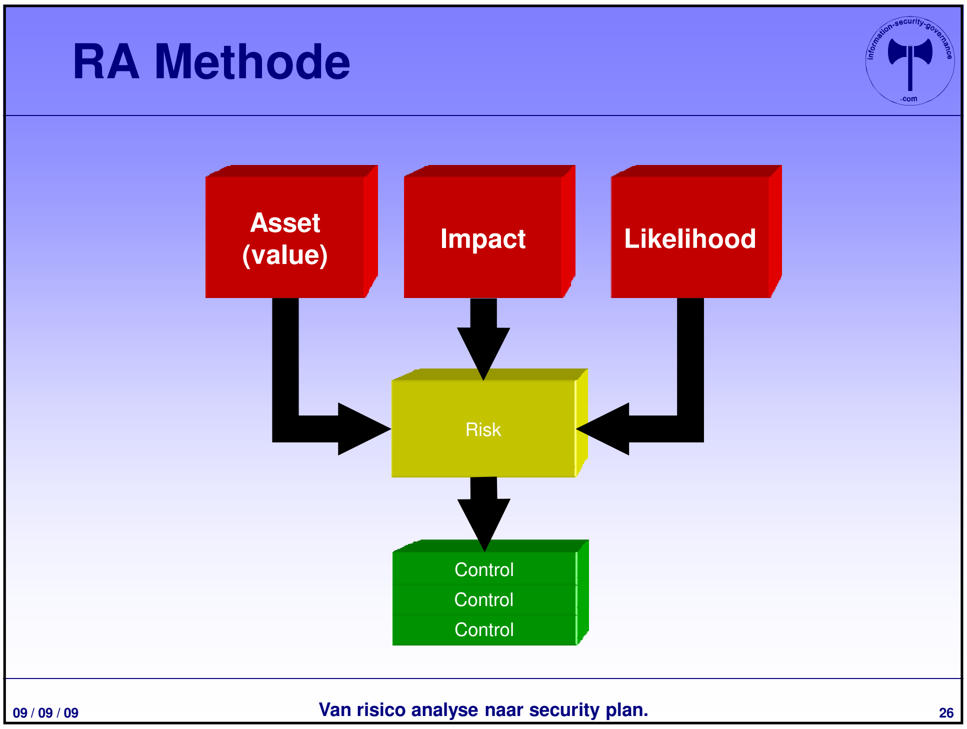


Impact & Likelihood

Likelihood	Definition
1	Less than twice a year
2	Between 3-5 times a year
3	Over 5 times a year

Impact	Definition
1	If the vulnerability is exploited, up to 33% of the asset will be lost
2	If the vulnerability is exploited, up to 66% of the asset will be lost
3	If the vulnerability is exploited, the asset will be completely lost

09 / 09 / 09 Van risico analyse naar security plan. 25



RA Methode

Asset (value)

Impact

Likelihood

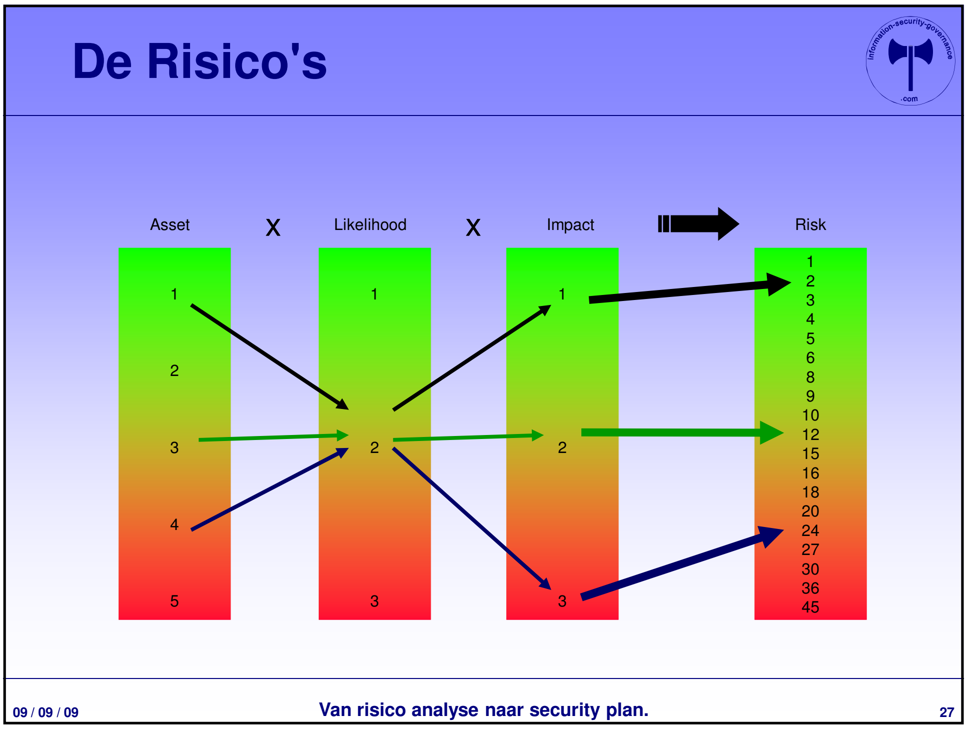
Risk

Control

Control

Control

09 / 09 / 09 Van risico analyse naar security plan. 26



De Risico's

Asset X Likelihood X Impact → Risk

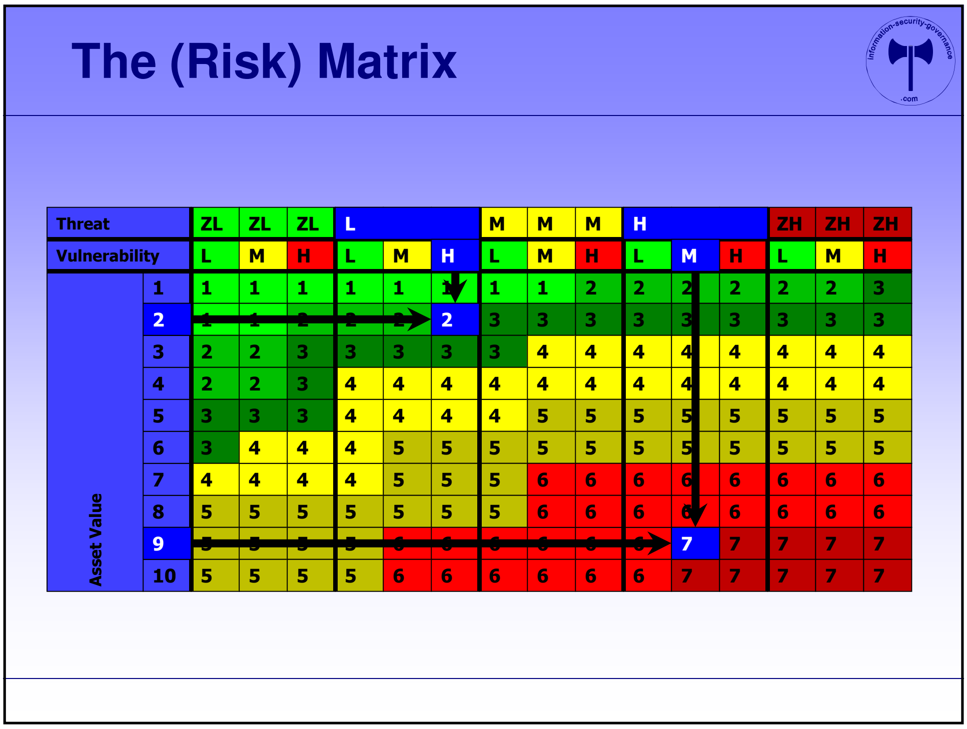
Asset: 1, 2, 3, 4, 5

Likelihood: 1, 2, 3

Impact: 1, 2, 3

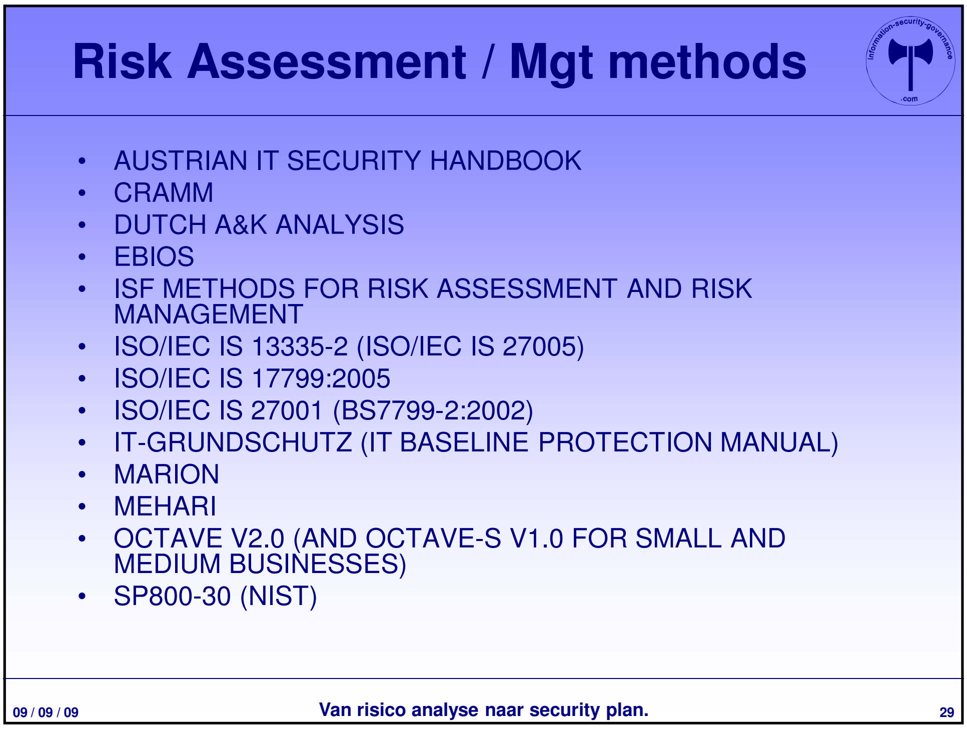
Risk: 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 27, 30, 36, 45

09 / 09 / 09 Van risico analyse naar security plan. 27



The (Risk) Matrix

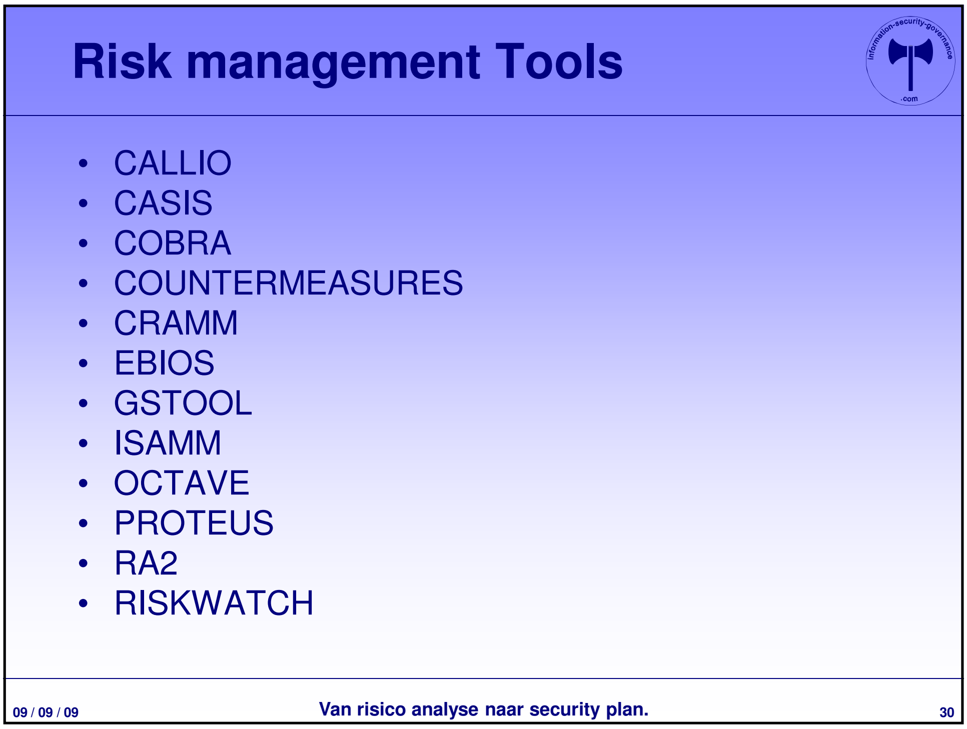
Threat		ZL	ZL	ZL	L			M	M	M	H			ZH	ZH	ZH
Vulnerability		L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
Asset Value	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	3
	2	1	1	2	2	2	2	3	3	3	3	3	3	3	3	3
	3	2	2	3	3	3	3	3	4	4	4	4	4	4	4	4
	4	2	2	3	4	4	4	4	4	4	4	4	4	4	4	4
	5	3	3	3	4	4	4	4	5	5	5	5	5	5	5	5
	6	3	4	4	4	5	5	5	5	5	5	5	5	5	5	5
	7	4	4	4	4	5	5	5	6	6	6	6	6	6	6	6
	8	5	5	5	5	5	5	5	6	6	6	6	6	6	6	6
	9	5	5	5	5	6	6	6	6	6	6	7	7	7	7	7
	10	5	5	5	5	6	6	6	6	6	6	7	7	7	7	7



Risk Assessment / Mgt methods

- AUSTRIAN IT SECURITY HANDBOOK
- CRAMM
- DUTCH A&K ANALYSIS
- EBIOS
- ISF METHODS FOR RISK ASSESSMENT AND RISK MANAGEMENT
- ISO/IEC IS 13335-2 (ISO/IEC IS 27005)
- ISO/IEC IS 17799:2005
- ISO/IEC IS 27001 (BS7799-2:2002)
- IT-GRUNDSCHUTZ (IT BASELINE PROTECTION MANUAL)
- MARION
- MEHARI
- OCTAVE V2.0 (AND OCTAVE-S V1.0 FOR SMALL AND MEDIUM BUSINESSES)
- SP800-30 (NIST)

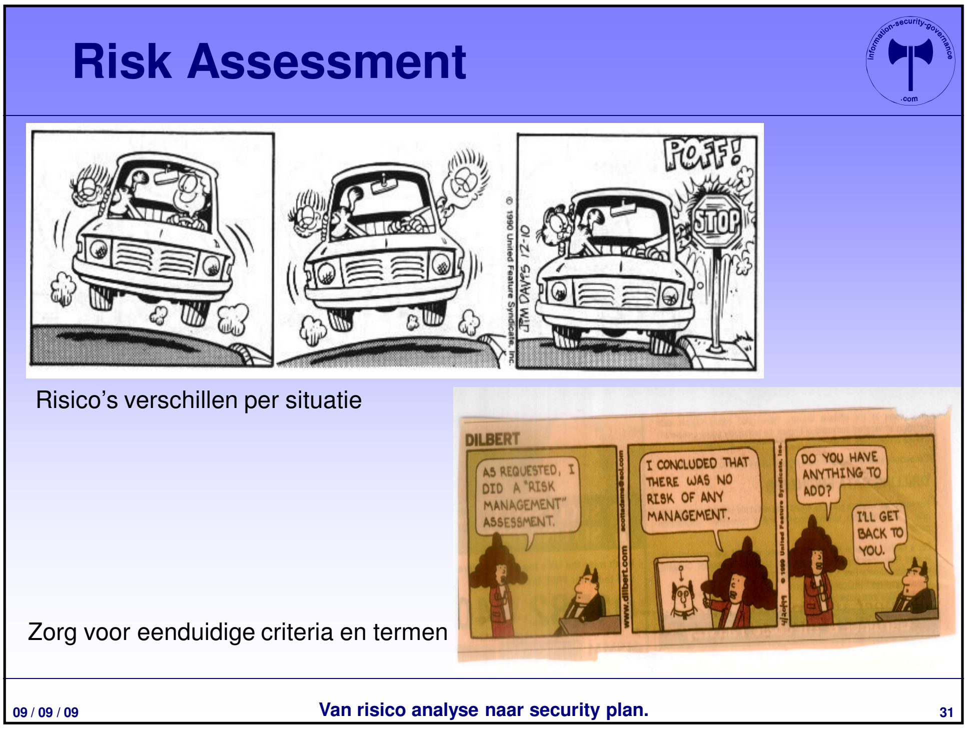
09 / 09 / 09 Van risico analyse naar security plan. 29



Risk management Tools

- CALLIO
- CASIS
- COBRA
- COUNTERMEASURES
- CRAMM
- EBIOS
- GSTOOL
- ISAMM
- OCTAVE
- PROTEUS
- RA2
- RISKWATCH

09 / 09 / 09 Van risico analyse naar security plan. 30



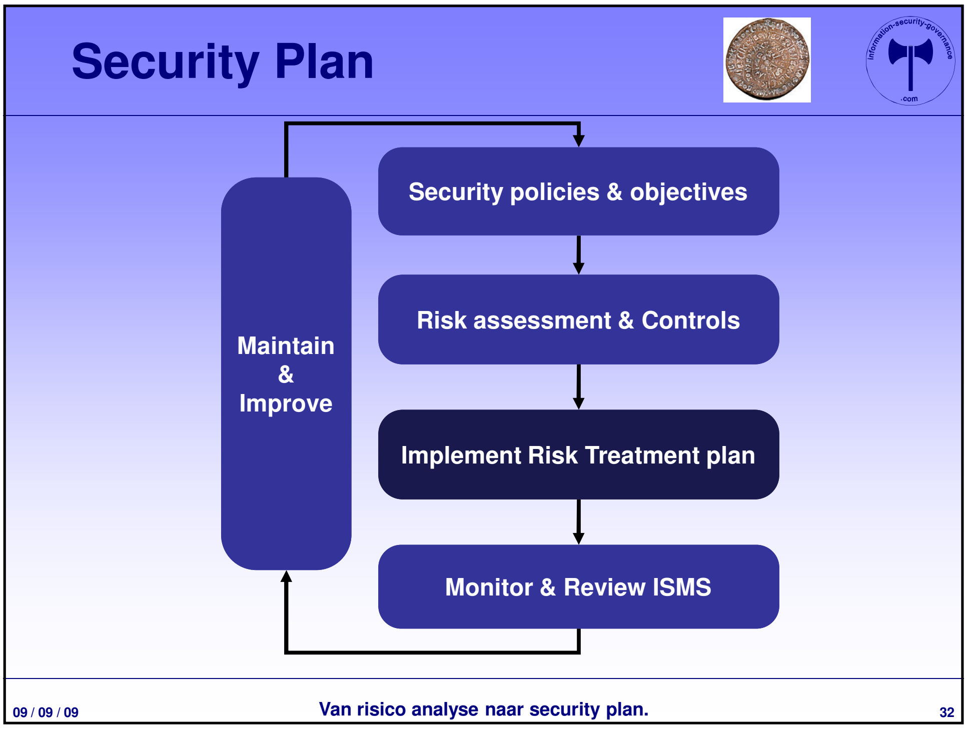
Risk Assessment

POFF!
STOP
DILBERT
AS REQUESTED, I DID A "RISK MANAGEMENT" ASSESSMENT.
I CONCLUDED THAT THERE WAS NO RISK OF ANY MANAGEMENT.
DO YOU HAVE ANYTHING TO ADD?
I'LL GET BACK TO YOU.

Risico's verschillen per situatie

Zorg voor eenduidige criteria en termen

09 / 09 / 09 Van risico analyse naar security plan. 31



Security Plan

Maintain & Improve

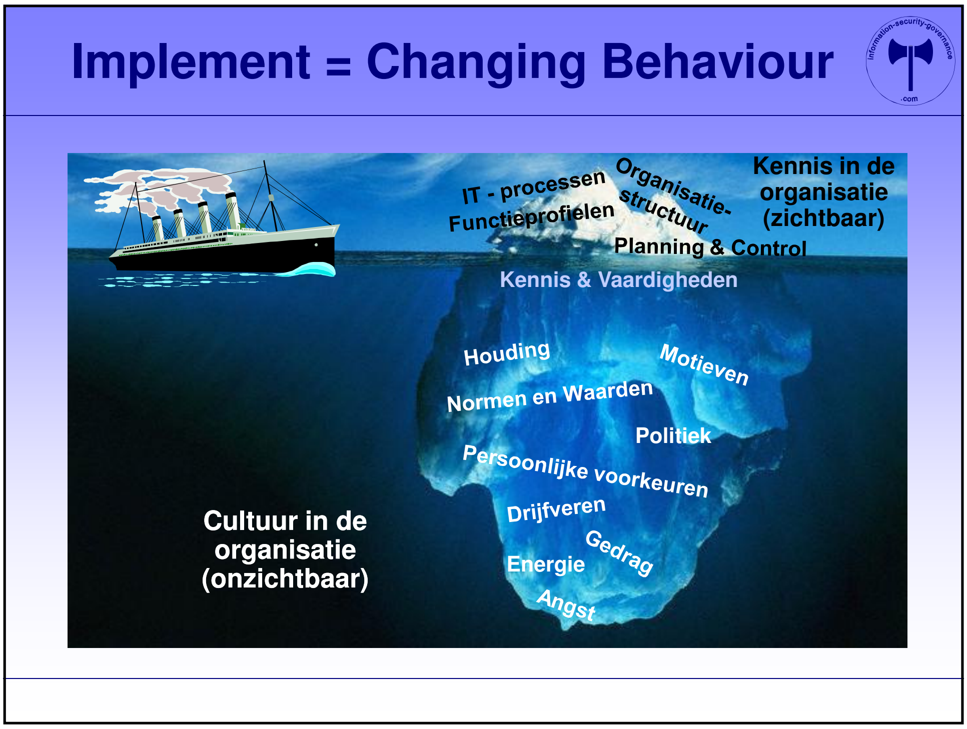
Security policies & objectives

Risk assessment & Controls

Implement Risk Treatment plan

Monitor & Review ISMS

09 / 09 / 09 Van risico analyse naar security plan. 32



Implement = Changing Behaviour

IT - processen
Functieprofielen
Organisatie-structuur
Planning & Control
Kennis in de organisatie (zichtbaar)
Kennis & Vaardigheden
Houding
Motieven
Normen en Waarden
Politiek
Persoonlijke voorkeuren
Drijfveren
Gedrag
Energie
Angst
Cultuur in de organisatie (onzichtbaar)

En dan is er… Beer Trial

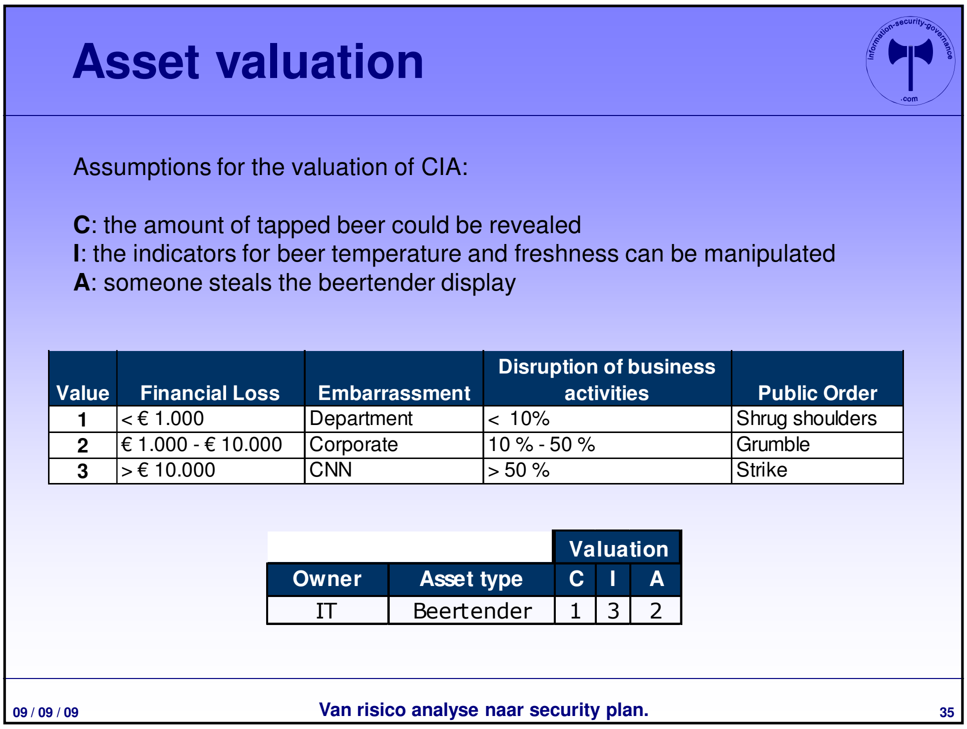
Volume Indicator: Shows how much beer is left in the keg

Freshness Indicator: Beer stays fresh 30 days from tapping

Temperature Indicator: Shows actual Beer temperature

Temperature Control: choose from 3 temperature settings.

09 / 09 / 09 Van risico analyse naar security plan. 34



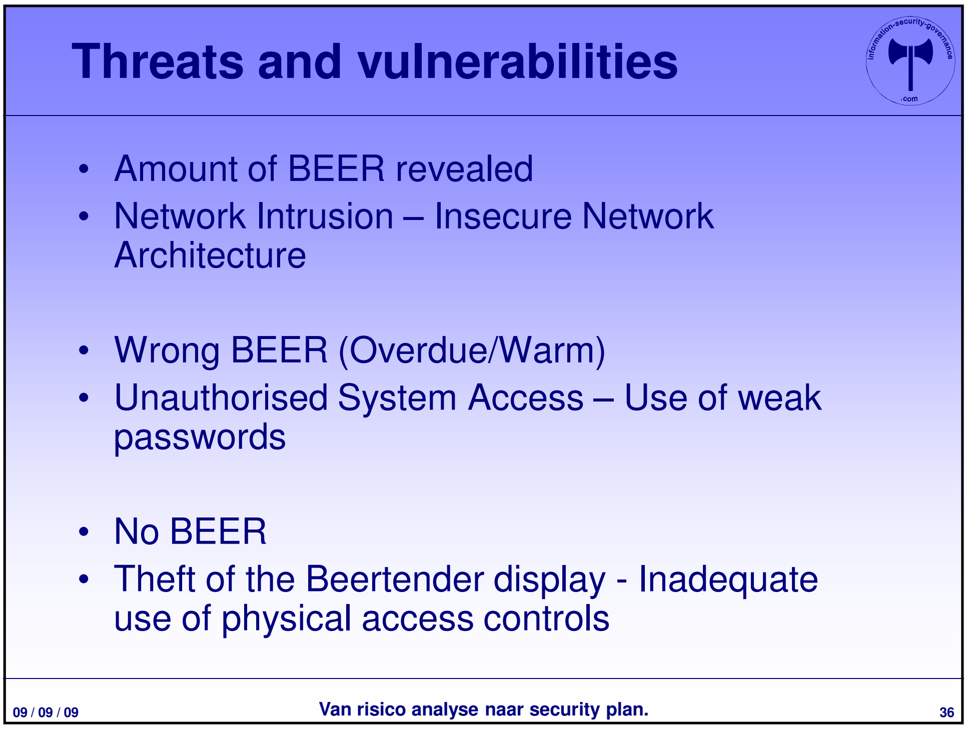
Asset valuation

Assumptions for the valuation of CIA:

C: the amount of tapped beer could be revealed
I: the indicators for beer temperature and freshness can be manipulated
A: someone steals the beertender display

Value	Financial Loss	Embarrassment	Disruption of business activities	Public Order
1	< € 1.000	Department	< 10%	Shrug shoulders
2	€ 1.000 - € 10.000	Corporate	10 % - 50 %	Grumble
3	> € 10.000	CNN	> 50 %	Strike

		Valuation		
Owner	Asset type	C	I	A
IT	Beertender	1	3	2

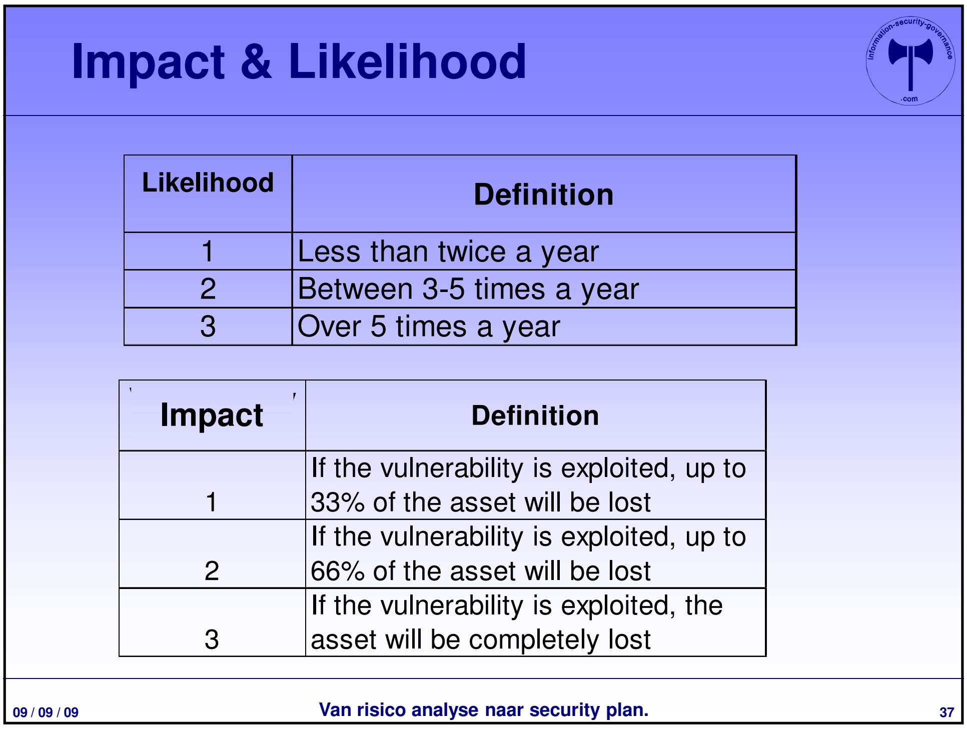


Threats and vulnerabilities

- Amount of BEER revealed
- Network Intrusion – Insecure Network Architecture

- Wrong BEER (Overdue/Warm)
- Unauthorised System Access – Use of weak passwords

- No BEER
- Theft of the Beertender display - Inadequate use of physical access controls

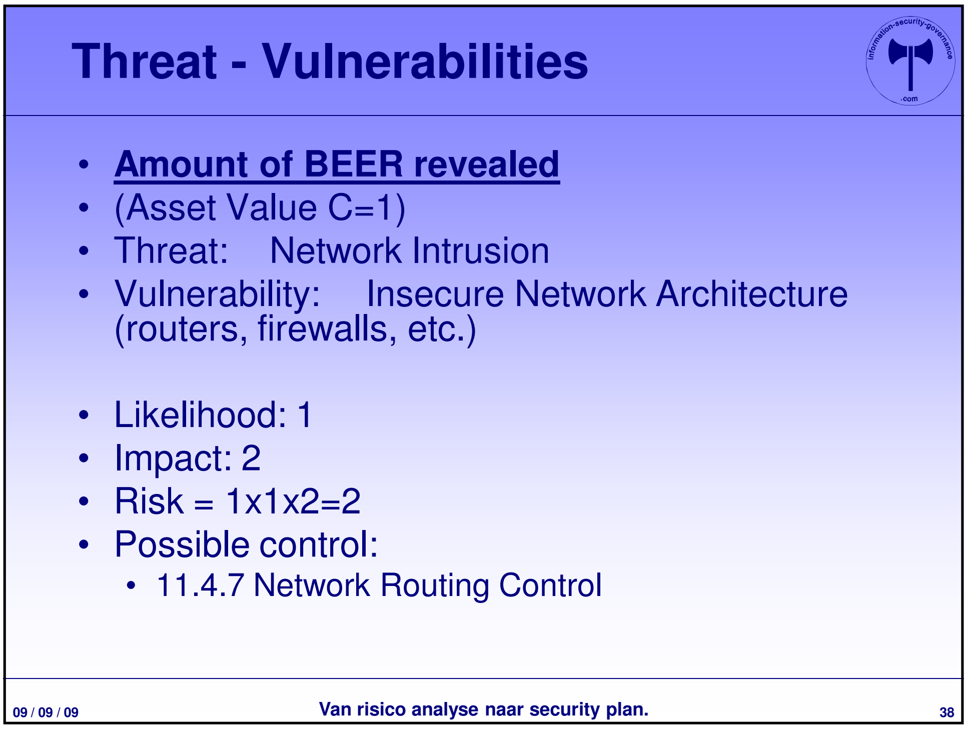


Impact & Likelihood

Likelihood	Definition
1	Less than twice a year
2	Between 3-5 times a year
3	Over 5 times a year

Impact	Definition
1	If the vulnerability is exploited, up to 33% of the asset will be lost
2	If the vulnerability is exploited, up to 66% of the asset will be lost
3	If the vulnerability is exploited, the asset will be completely lost

09 / 09 / 09 Van risico analyse naar security plan. 37

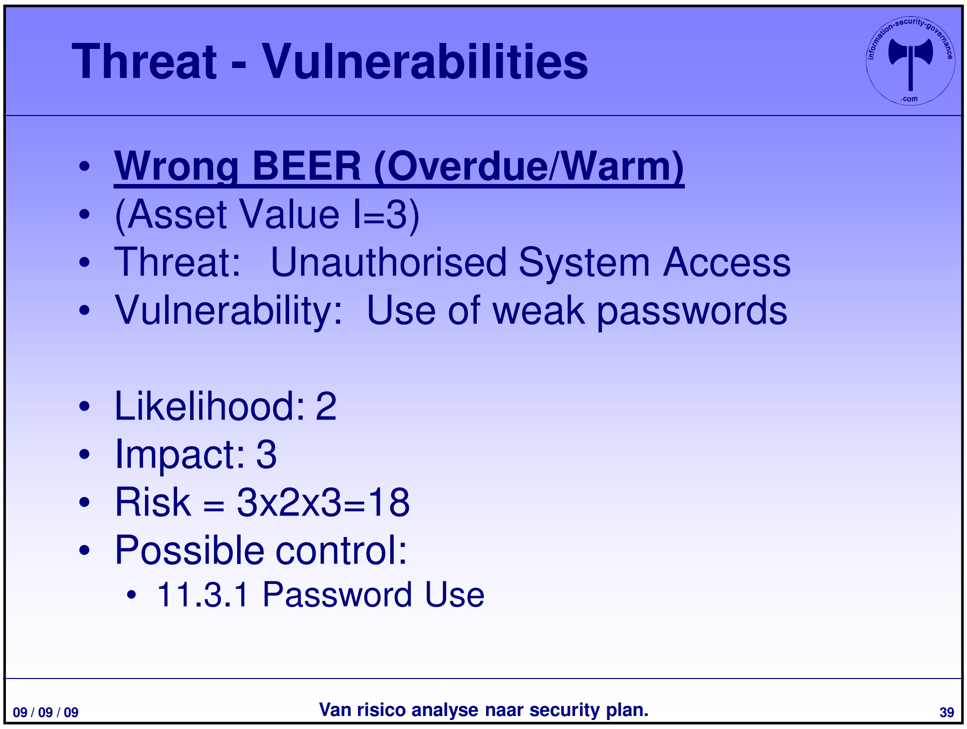


Threat - Vulnerabilities

- **Amount of BEER revealed**
- (Asset Value C=1)
- Threat: Network Intrusion
- Vulnerability: Insecure Network Architecture (routers, firewalls, etc.)

- Likelihood: 1
- Impact: 2
- Risk = 1x1x2=2
- Possible control:
  - 11.4.7 Network Routing Control

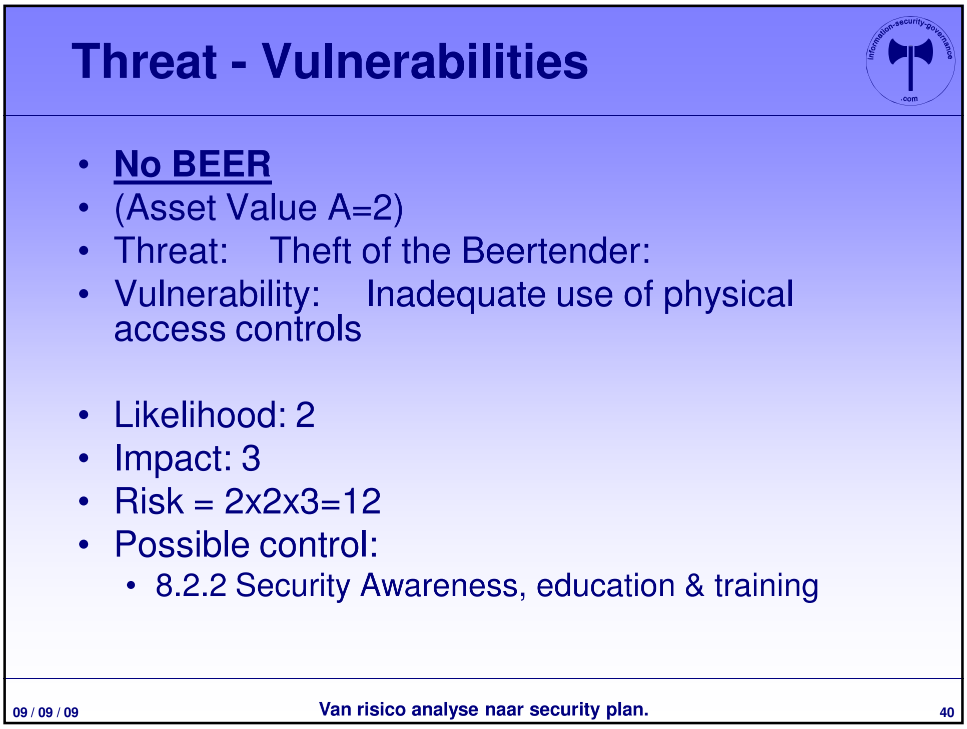
09 / 09 / 09 Van risico analyse naar security plan. 38



Threat - Vulnerabilities

- **Wrong BEER (Overdue/Warm)**
- (Asset Value I=3)
- Threat: Unauthorised System Access
- Vulnerability: Use of weak passwords

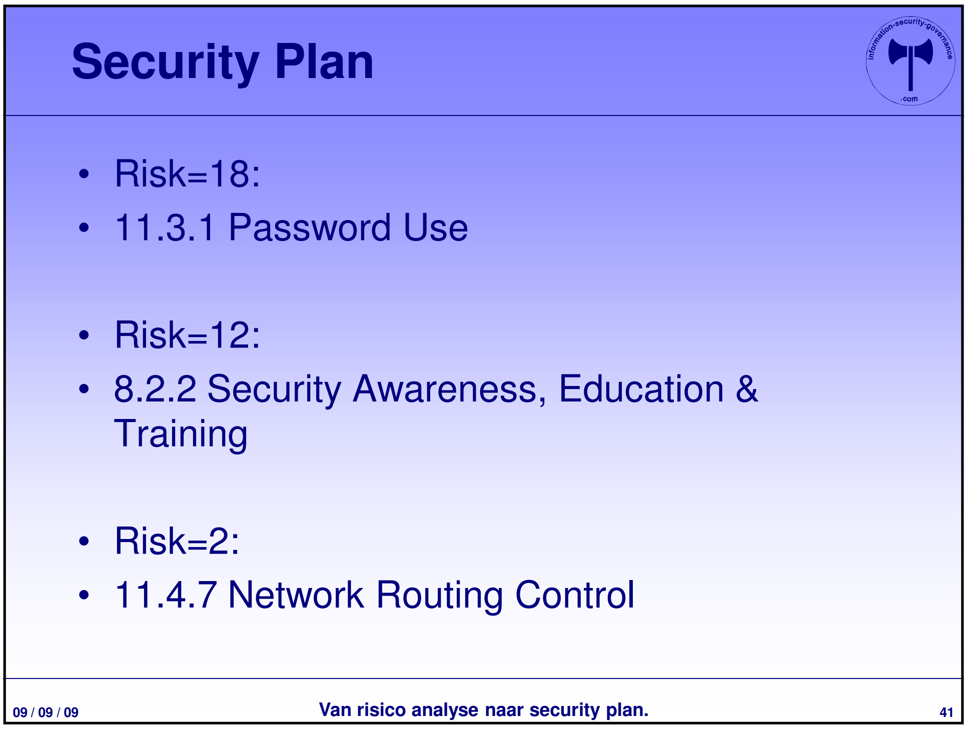
- Likelihood: 2
- Impact: 3
- Risk = 3x2x3=18
- Possible control:
  - 11.3.1 Password Use



Threat - Vulnerabilities

- **No BEER**
- (Asset Value A=2)
- Threat: Theft of the Beertender:
- Vulnerability: Inadequate use of physical access controls

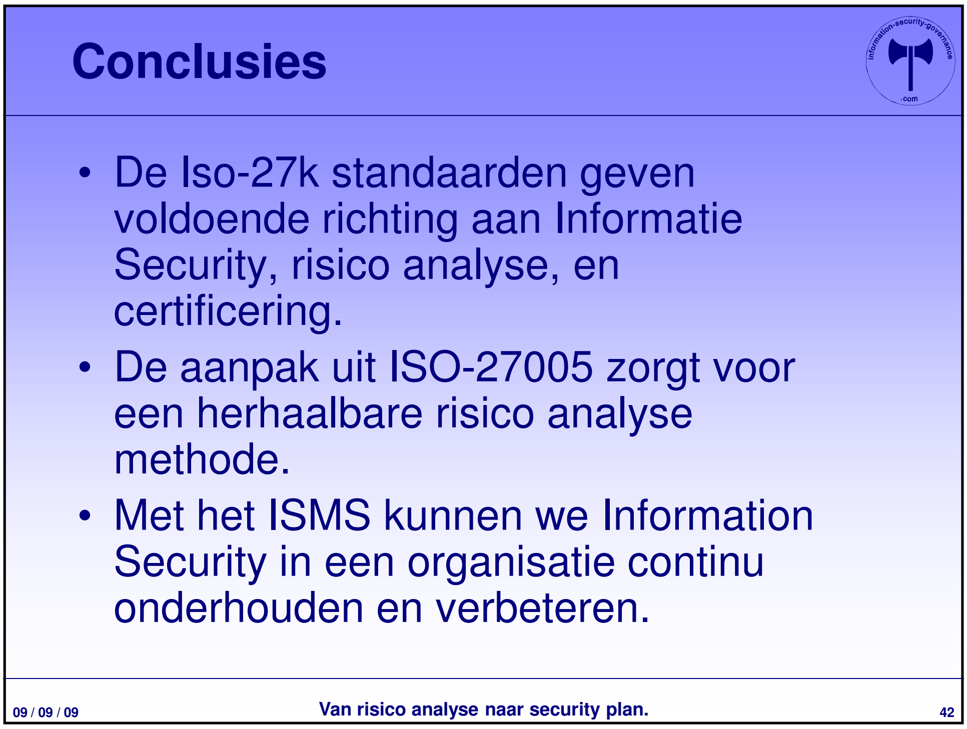
- Likelihood: 2
- Impact: 3
- Risk = 2x2x3=12
- Possible control:
  - 8.2.2 Security Awareness, education & training



Security Plan

- Risk=18:
- 11.3.1 Password Use
- Risk=12:
- 8.2.2 Security Awareness, Education & Training
- Risk=2:
- 11.4.7 Network Routing Control

09 / 09 / 09 Van risico analyse naar security plan. 41



Conclusies

- De Iso-27k standaarden geven voldoende richting aan Informatie Security, risico analyse, en certificering.
- De aanpak uit ISO-27005 zorgt voor een herhaalbare risico analyse methode.
- Met het ISMS kunnen we Information Security in een organisatie continu onderhouden en verbeteren.

09 / 09 / 09 Van risico analyse naar security plan. 42

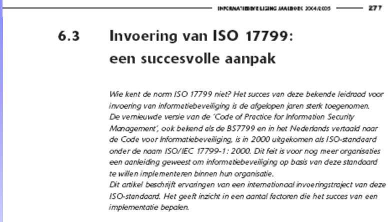
ISO-27000 Information Security

“That's one small step for a man, a giant leap for mankind.”

Neil Armstrong, Apollo 11, 21 july 1969

09 / 09 / 09 Van risico analyse naar security plan. 43

Readings

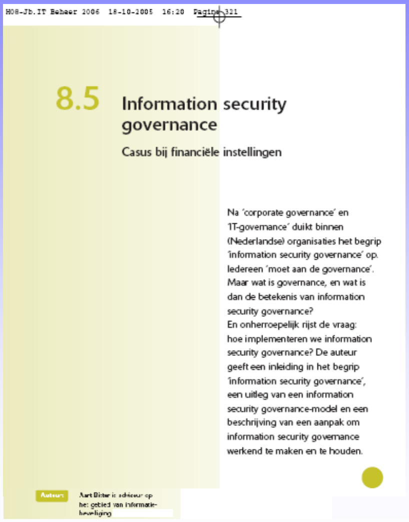


INFORMATIEBEVEILIGING JAARBOEK 2004/2005 277

6.3 Invoering van ISO 17799: een succesvolle aanpak

Wie kent de norm ISO 17799 niet? Het succes van deze bekende leidraad voor invoering van informatiebeveiliging is de afgelopen jaren sterk toegenomen. De vernieuwde versie van de 'Code of Practice for Information Security Management', ook bekend als de BS7799 en in het Nederlands vertaald naar de Code voor Informatiebeveiliging, is in 2000 uitgekomen als ISO-standaard onder de naam ISO/IEC 17799-1: 2000. Dit feit is voor nog meer organisaties een aanleiding geweest om informatiebeveiliging op basis van deze standaard te willen implementeren binnen hun organisatie.

Dit artikel beschrijft ervaringen van een internationaal invoeringstraject van deze ISO-standaard. Het geeft inzicht in een aantal factoren die het succes van een implementatie bepalen.



H08-Jb.IT Beheer 2006 18-10-2005 16:20 Pagina 321

8.5 Information security governance

Casus bij financiële instellingen

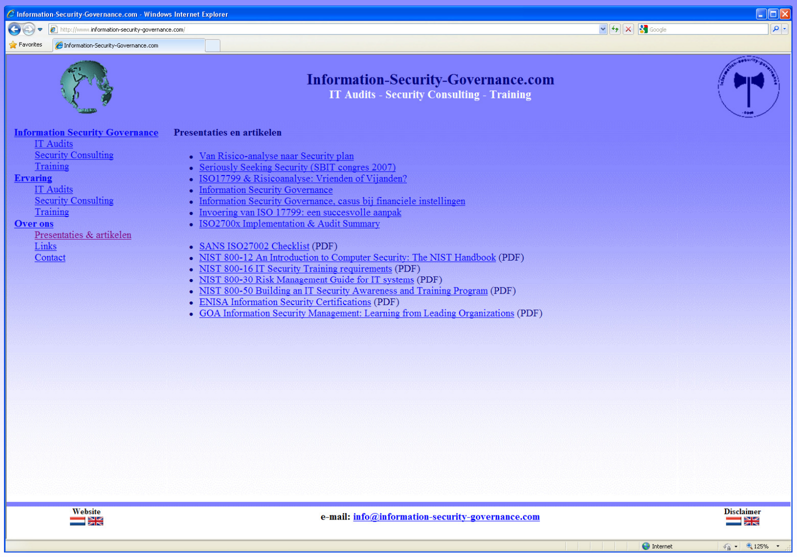
Na 'corporate governance' en 'IT-governance' duikt binnen (Nederlandse) organisaties het begrip 'information security governance' op. Iedereen 'moet aan de governance'. Maar wat is governance, en wat is dan de betekenis van information security governance?

En onherroepelijk rijst de vraag: hoe implementeren we information security governance? De auteur geeft een inleiding in het begrip 'information security governance', een uitleg van een information security governance-model en een beschrijving van een aanpak om information security governance werkend te maken en te houden.

Auteur: Aart Bitter is adviseur op het gebied van informatie-beveiliging

09 / 09 / 09 Van risico analyse naar security plan. 44

Further reference



Information-Security-Governance.com - Windows Internet Explorer
http://www.information-security-governance.com/
Google
Favorites
Information-Security-Governance.com
Internet
125%

Information-Security-Governance.com

IT Audits - Security Consulting - Training

- **Information Security Governance**
  - IT Audits
  - Security Consulting
  - Training
- **Ervaring**
  - IT Audits
  - Security Consulting
  - Training
- **Over ons**
  - Presentaties & artikelen
  - Links
  - Contact

Presentaties en artikelen

- Van Risico-analyse naar Security plan
- Seriously Seeking Security (SBIT congres 2007)
- ISO17799 & Risicoanalyse: Vrienden of Vijanden?
- Information Security Governance
- Information Security Governance, casus bij financiele instellingen
- Invoering van ISO 17799: een succesvolle aanpak
- ISO2700x Implementation & Audit Summary

- SANS ISO27002 Checklist (PDF)
- NIST 800-12 An Introduction to Computer Security: The NIST Handbook (PDF)
- NIST 800-16 IT Security Training requirements (PDF)
- NIST 800-30 Risk Management Guide for IT systems (PDF)
- NIST 800-50 Building an IT Security Awareness and Training Program (PDF)
- ENISA Information Security Certifications (PDF)
- GOA Information Security Management: Learning from Leading Organizations (PDF)

Website

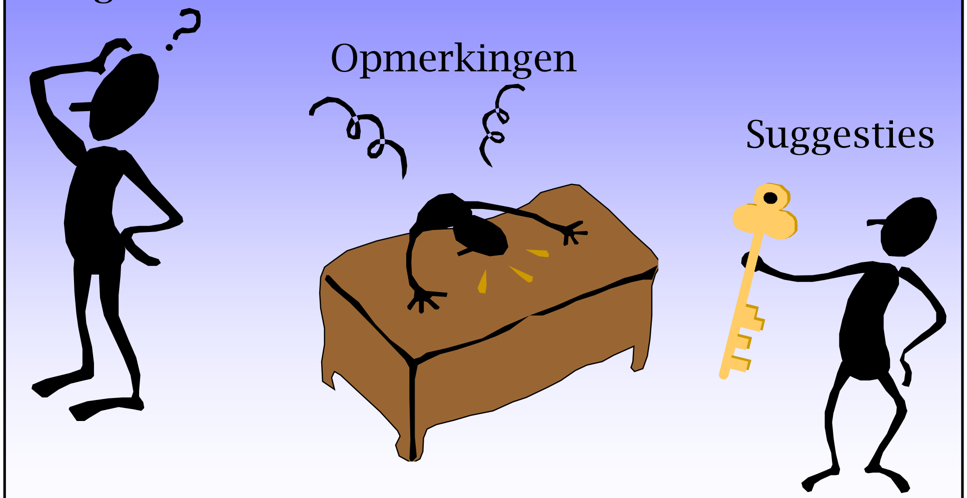
e-mail: info@information-security-governance.com

Disclaimer

09 / 09 / 09 Van risico analyse naar security plan. 45

Dank voor uw aandacht !

Vragen



Opmerkingen

Suggesties

www.information-security-governance.com

09 / 09 / 09 Van risico analyse naar security plan. 46