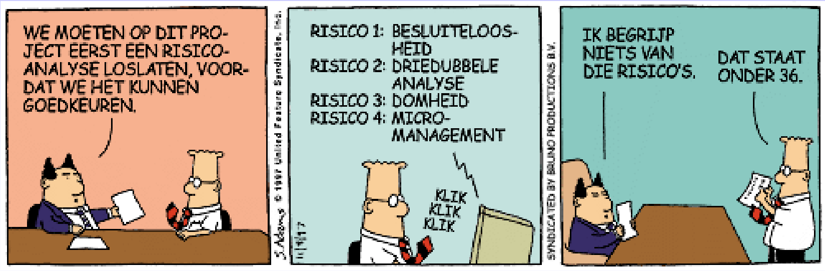
ISO17799 & Risicoanalyse: Vrienden of Vijanden?

Aart Bitter
20 september 2007

Aart.Bitter@information-security-governance.com

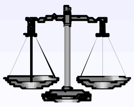
Agenda

- Hoe wordt een goede risico analyse uitgevoerd?
- Risico's – maatregelen - incidenten

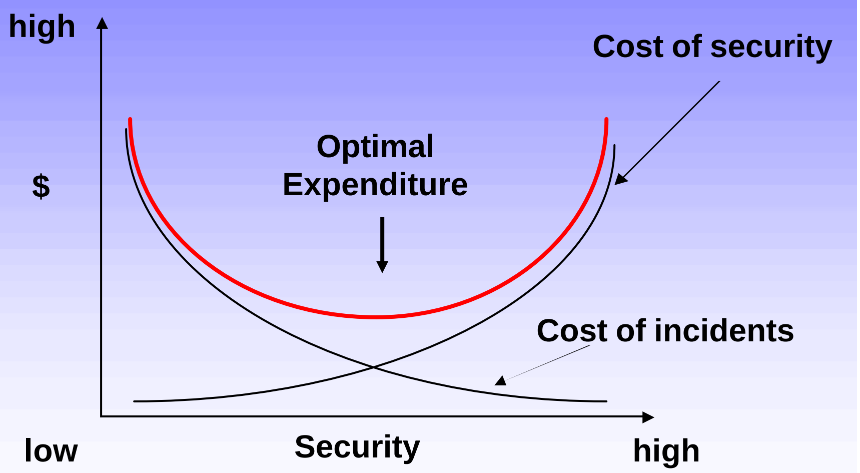

WE MOETEN OP DIT PROJECT EERST EEN RISICO-ANALYSE LOSLATEN, VOORDAT WE HET KUNNEN GOEDKEUREN.
S.Adams © 1997 United Feature Syndicate, Inc.
RISICO 1: BESLUITELOOSHEID
RISICO 2: DRIEDUBBELE ANALYSE
RISICO 3: DOMHEID
RISICO 4: MICRO-MANAGEMENT
KLIK KLIK KLIK
SYNDICATED BY BRUNO PRODUCTIONS B.V.
IK BEGRIJP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

Vijand

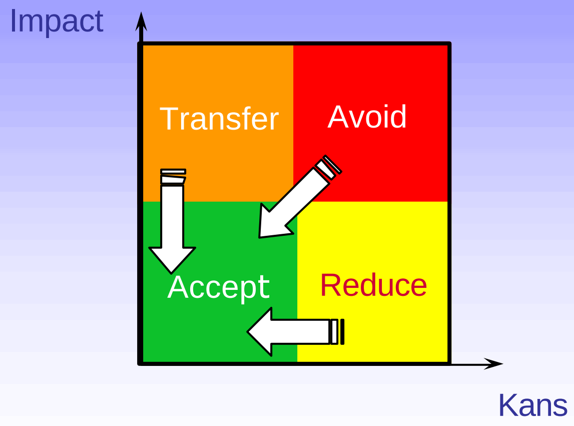
- Het niet beheersen van beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening zal leiden tot:
  - Verlies van vertrouwen bij klanten en het niet kunnen doen van “nieuwe business”
  - Juridische straffen (rechtszaken)
  - Onnodig extra werk / beheer
  - Het niet kunnen garanderen van de continuïteit van de bedrijfsvoering
- Verdediging: informatiebeveiliging / Information Security
- Wat beveiligen, Hoeveel beveiligen



Wat en hoeveel: Risicoanalyse



Risico management



Impact

Transfer

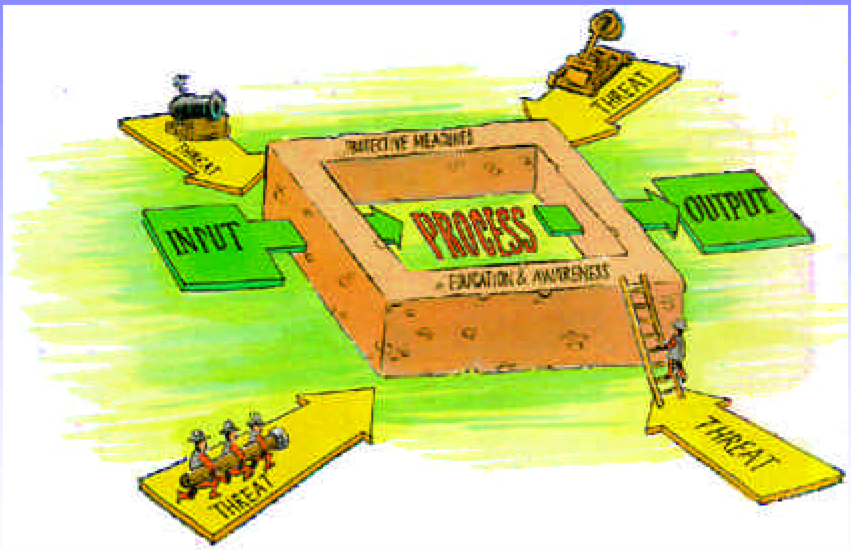
Avoid

Accept

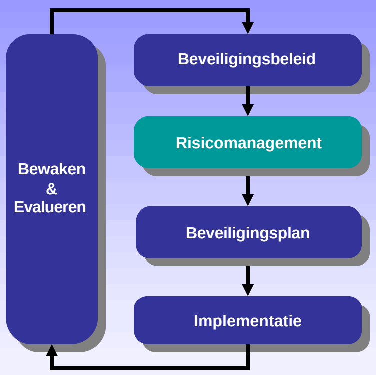
Reduce

Kans

Security Management



Informatiebeveiligingsmodel



2006 Survey of RM/RA

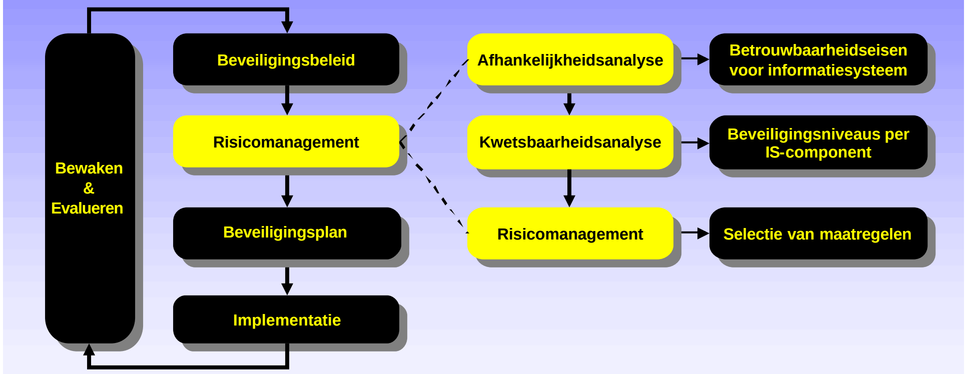
Methodes

- Australian IT Security handbook
- **CRAMM**
- **Dutch A&K analysis**
- EBIOS
- ISF methods for RA & RM
- **ISO/IEC 13335-2 (ISO/IEC 27005)**
- **ISO/IEC 17799:2005**
- **ISO/IEC 27001**
- IT Baseline Protection Manual
- MARION
- HEHARI
- Octave v2.0
- SP800-30 (NIST)

Tools

- Callio
- Casis
- Cobra
- CounterMeasures
- CRAMM
- EBIOS
- GSTool
- ISAMM
- Octave
- Proteus
- RA2
- RiskWatch

Risico (A&K) analyse



Bewaken & Evalueren

Beveiligingsbeleid

Risicomanagement

Beveiligingsplan

Implementatie

Afhankelijkheidsanalyse

Kwetsbaarheidsanalyse

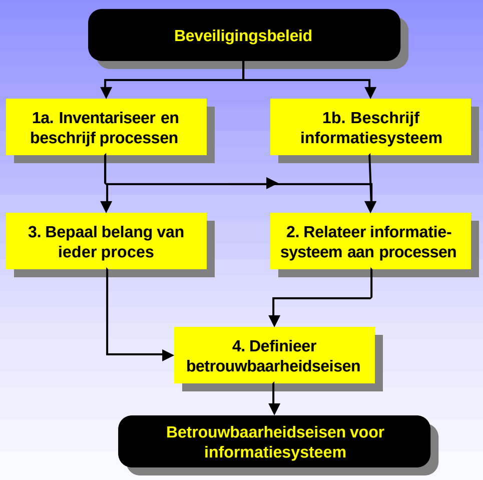
Risicomanagement

Betrouwbaarheidseisen voor informatiesysteem

Beveiligingsniveaus per IS-component

Selectie van maatregelen

Afhankelijkheidsanalyse



Beveiligingsbeleid

1a. Inventariseer en beschrijf processen

1b. Beschrijf informatiesysteem

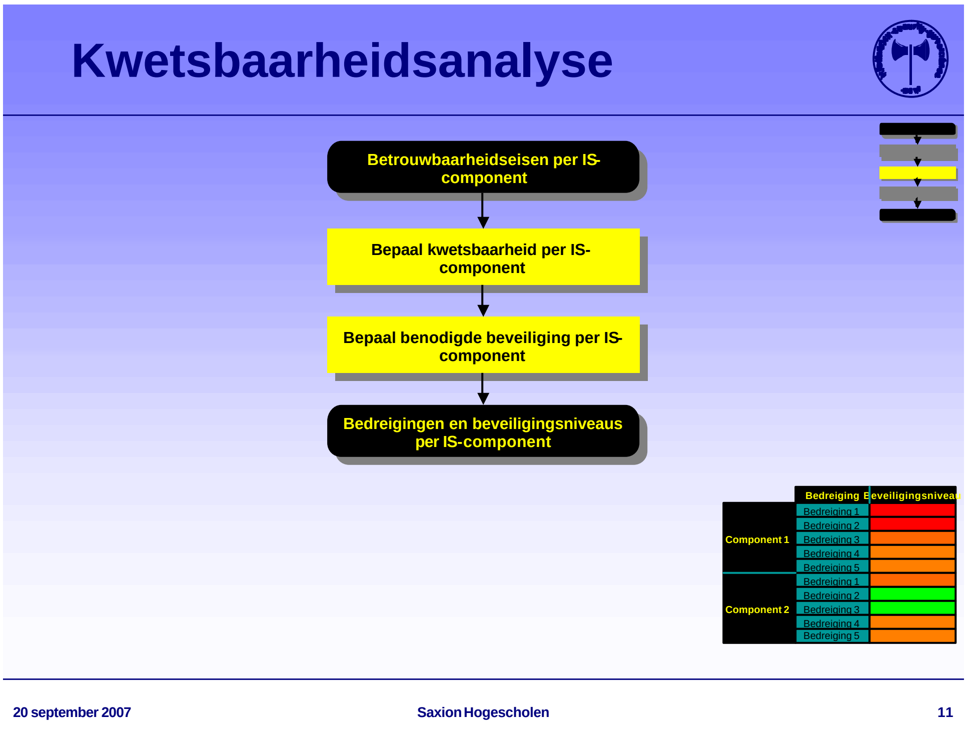
3. Bepaal belang van ieder proces

2. Relateer informatie-systeem aan processen

4. Definieer betrouwbaarheidseisen

Betrouwbaarheidseisen voor informatiesysteem

	Betrouwbaarheidseis		
	B	I	V
IS1	H	L	M
IS2	L	H	M



Kwetsbaarheidsanalyse

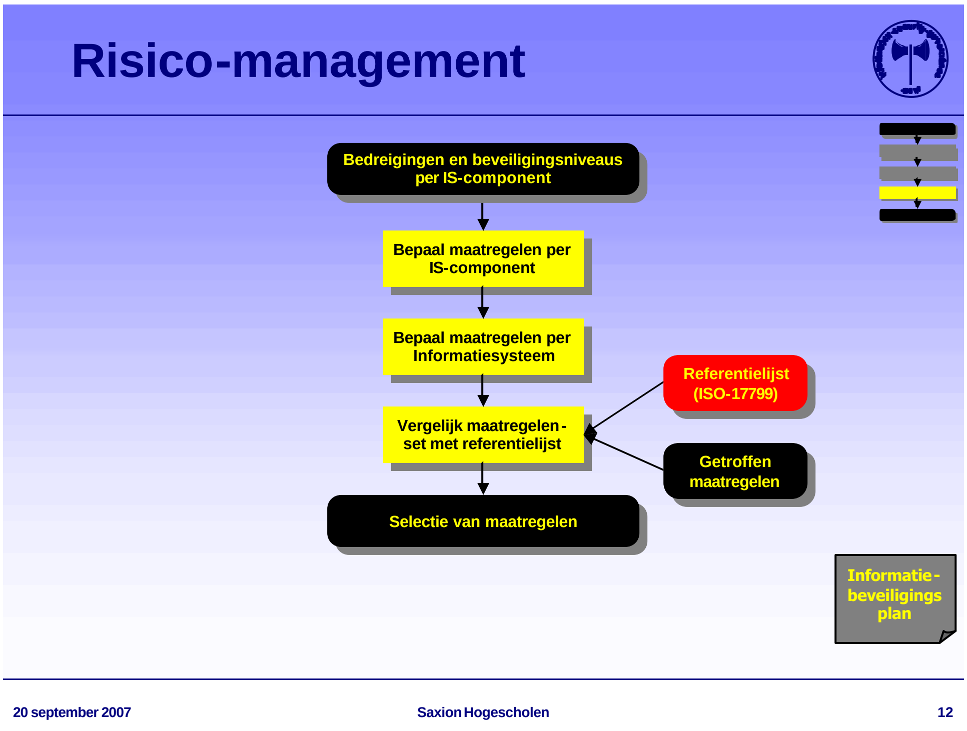
Betrouwbaarheidseisen per IS-component

Bepaal kwetsbaarheid per IS-component

Bepaal benodigde beveiliging per IS-component

Bedreigingen en beveiligingsniveaus per IS-component

	Bedreiging	Beveiligingsniveau
Component 1	Bedreiging 1	🟥
	Bedreiging 2	🟥
	Bedreiging 3	🟧
	Bedreiging 4	🟧
	Bedreiging 5	🟧
Component 2	Bedreiging 1	🟧
	Bedreiging 2	🟩
	Bedreiging 3	🟩
	Bedreiging 4	🟧
	Bedreiging 5	🟧



Risico-management

Bedreigingen en beveiligingsniveaus per IS-component

Bepaal maatregelen per IS-component

Bepaal maatregelen per Informatiesysteem

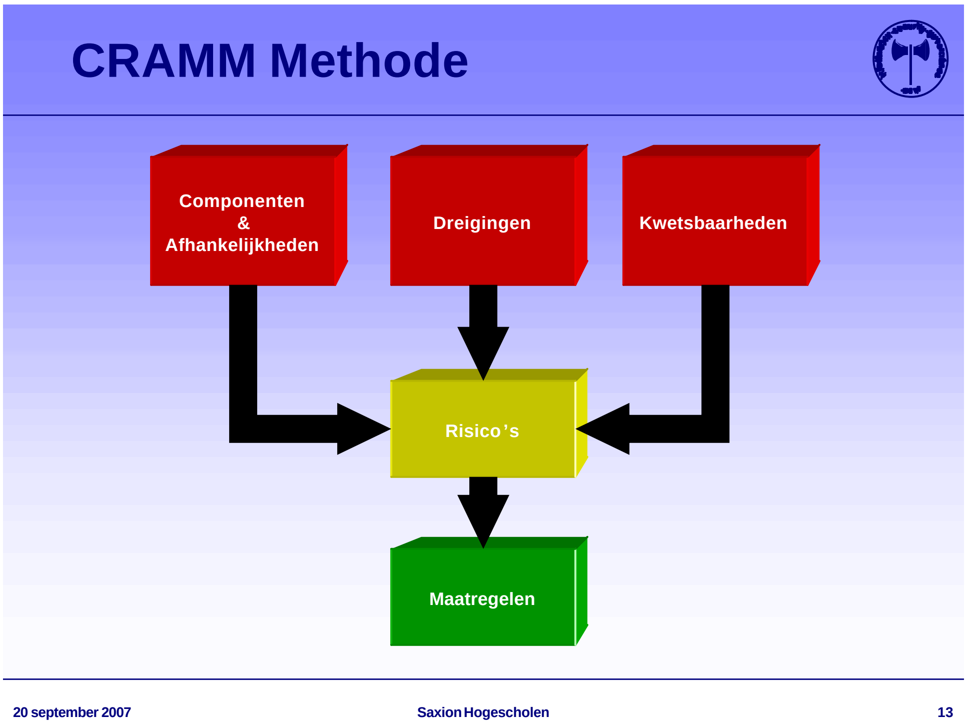
Vergelijk maatregelen-set met referentielijst

Referentielijst (ISO-17799)

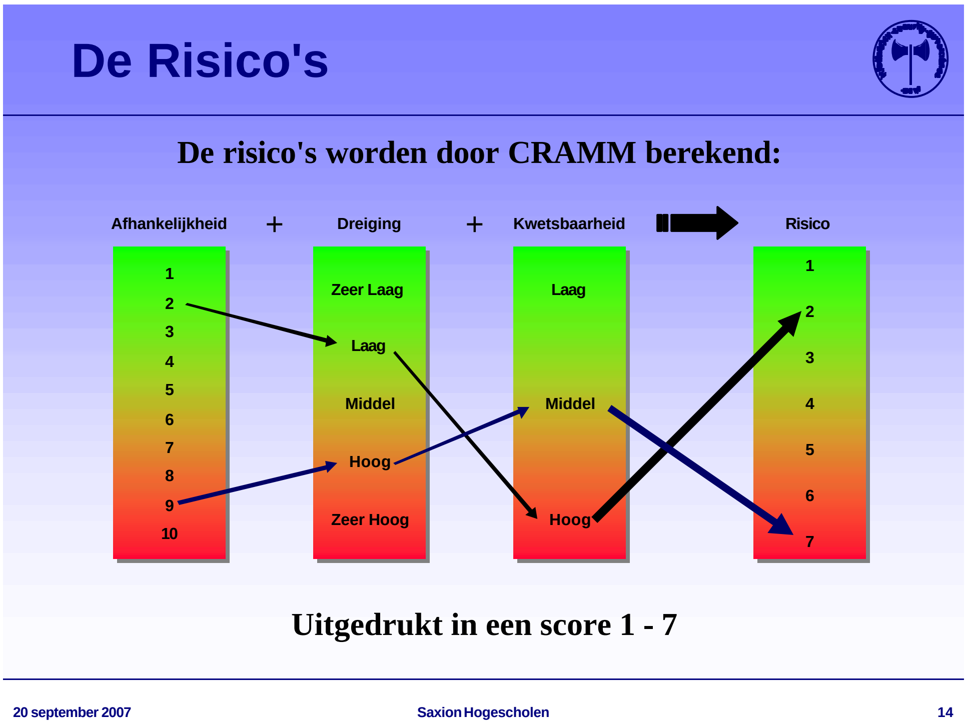
Getroffen maatregelen

Selectie van maatregelen

Informatie-beveiligings plan



CRAMM Methode

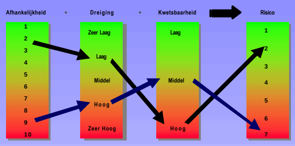


De Risico's

De risico's worden door CRAMM berekend:

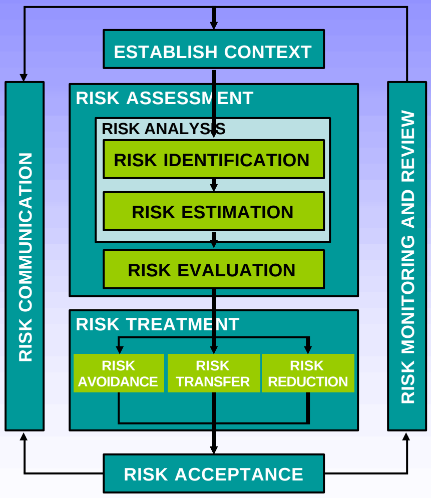
Uitgedrukt in een score 1 - 7

De Risico-matrix



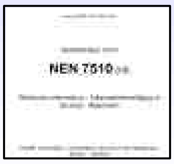
	Dreiging	ZL	ZL	ZL	L			M	M	M	H			ZH	ZH	ZH
	Kwetsbaarheid	L	M	H	L	M	H	L	M	H	L	M	H	L	M	H
Afhankelijkheid	1	1	1	1	1	1	[illegible]	1	1	2	2	2	2	2	2	3
	2	1	1	2	2	2	2	3	3	3	3	3	3	3	3	3
	3	2	2	3	3	3	3	3	4	4	4	4	4	4	4	4
	4	2	2	3	4	4	4	4	4	4	4	4	4	4	4	4
	5	3	3	3	4	4	4	4	5	5	5	5	5	5	5	5
	6	3	4	4	4	5	5	5	5	5	5	5	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	[illegible]	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

ISO-27005 Risk Assessment & Treatment



ORGANISATION INTERNATIONALE DE NORMALISATION

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION



INTERNATIONAL STANDARD

ISO/IEC 17799

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

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

ISMS Definition

- An ISMS (**Information Security Management System**) is the part of the overall management system that, based on a business **risk** approach, is intended to ensure the **availability, confidentiality** and **integrity** of information and associated assets.

4.2.1 Establish the ISMS (2/5)

c) Define a systematic approach to risk assessment

1) Identify a method of risk assessment that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.

2) Determine criteria for accepting the risks and identify the acceptable levels of risk

The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results.

d) Identify the risks

1) Identify the assets and the owners of these assets.

2) Identify the threats to those assets.

3) Identify the vulnerabilities that might be exploited by the threats.

4) Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

4.2.1 Establish the ISMS (3/5)

e) Assess the risks

1) Assess the business harm that might result from a security failure

2) Assess the realistic likelihood of such a security failure

3) Estimate the levels of risks.

4) Determine whether the risk is acceptable or requires treatment using the criteria established in c).

f) Identify and evaluate options for the treatment of risks

Possible actions include:

1) applying appropriate controls;

2) knowingly and objectively accepting risks

3) avoiding risks;

4) transferring the associated business risks to other parties, e.g. insurers, suppliers.

4.2.1 Establish the ISMS (4/5)

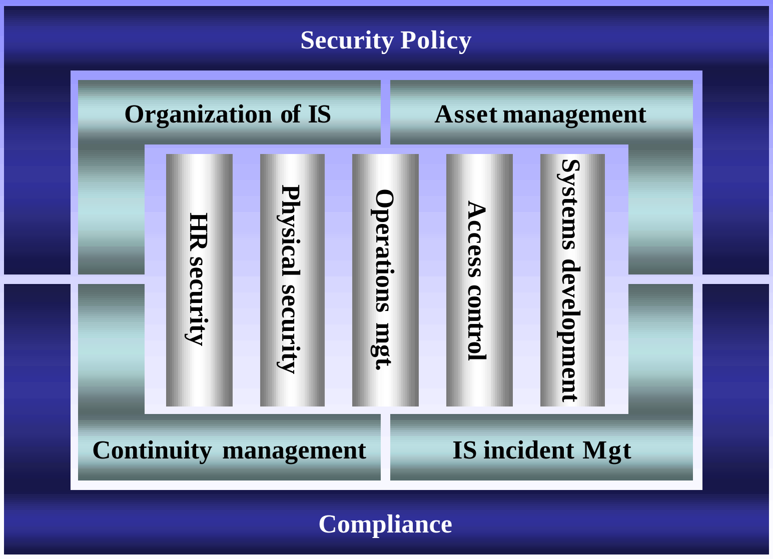
g) Select control objectives and controls for the treatment of risks

Control objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection shall take account of the criteria for accepting risks (see 4.2.1c)2)) as well as legal, regulatory and contractual requirements.

The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover the identified requirements.

The control objectives and controls listed in Annex A are not exhaustive and additional control objectives and controls may also be selected.

ISO/IEC 17799



Security Policy

Organization of IS

Asset management

HR security

Physical security

Operations mgt.

Access control

Systems development

Continuity management

IS incident Mgt

Compliance

So far, so good

ISO 27000 – ***principles and vocabulary***

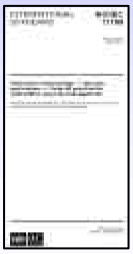
ISO 27001 – **ISMS requirements**

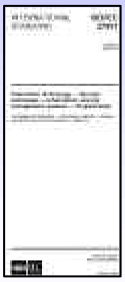
ISO 27002 – *(ISO/ IEC 17799:2005)*

ISO 27003 – ***ISMS Implementation guidelines***

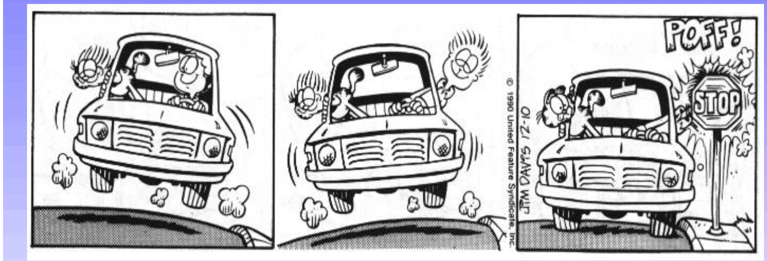
ISO 27004 – ***ISMS Metrics and measurement***

ISO 27005 – ***ISMS Risk Management***





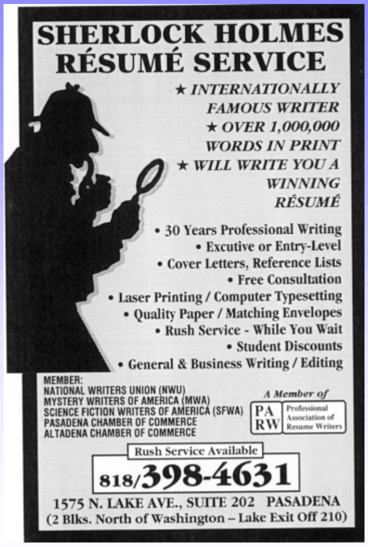
Risk Assessment



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.

Security Policy

Organization of Info. Security



SHERLOCK HOLMES
RÉSUMÉ SERVICE

★ INTERNATIONALLY FAMOUS WRITER
★ OVER 1,000,000 WORDS IN PRINT
★ WILL WRITE YOU A WINNING RÉSUMÉ

- 30 Years Professional Writing
- Excutive or Entry-Level
- Cover Letters, Reference Lists
- Free Consultation
- Laser Printing / Computer Typesetting
- Quality Paper / Matching Envelopes
- Rush Service - While You Wait
- Student Discounts
- General & Business Writing / Editing

MEMBER:
NATIONAL WRITERS UNION (NWU)
MYSTERY WRITERS OF AMERICA (MWA)
SCIENCE FICTION WRITERS OF AMERICA (SFWA)
PASADENA CHAMBER OF COMMERCE
ALTADENA CHAMBER OF COMMERCE

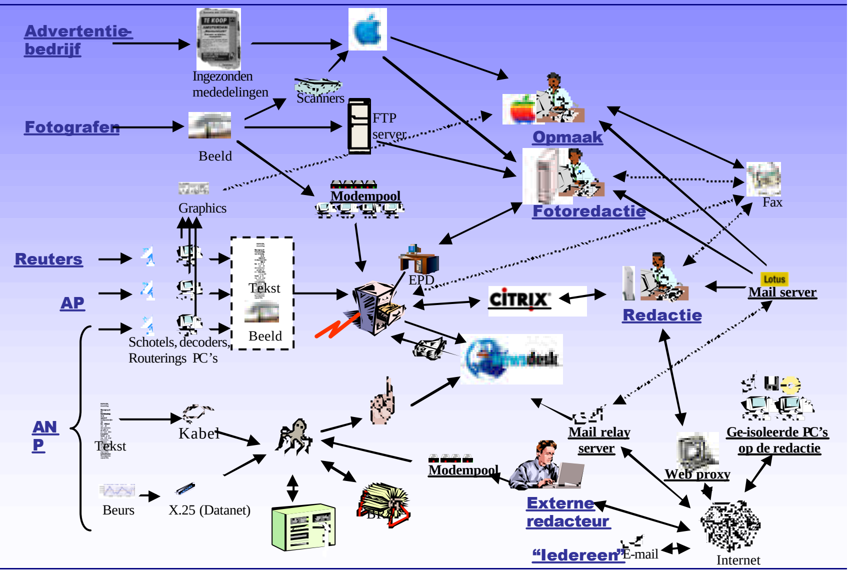
A Member of
PA RW Professional Association of Resume Writers

Rush Service Available

818/398-4631

1575 N. LAKE AVE., SUITE 202 PASADENA
(2 Blks. North of Washington – Lake Exit Off 210)

Asset management



Advertentie-bedrijf

Ingezonden mededelingen

Scanners

FTP server

Fotografen

Beeld

Graphics

Modempool

Opmaak

Fotoredactie

Fax

Reuters

AP

Tekst

Beeld

Schotels, decoders, Routerings PC's

EPD

CITRIX

Redactie

Lotus

Mail server

ANP

Tekst

Kabel

Beurs

X.25 (Datanet)

BRS

Modempool

Mail relay server

Web proxy

Ge-isoleerde PC's op de redactie

Externe redacteur

"Iedereen"

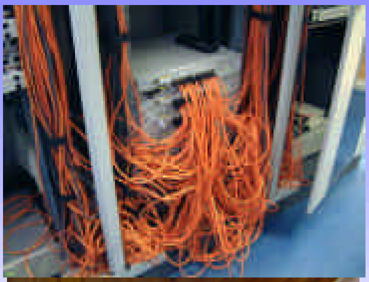
E-mail

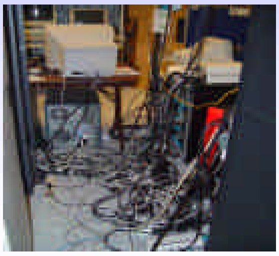
Internet

Human Resources Security

Physical Security (1)

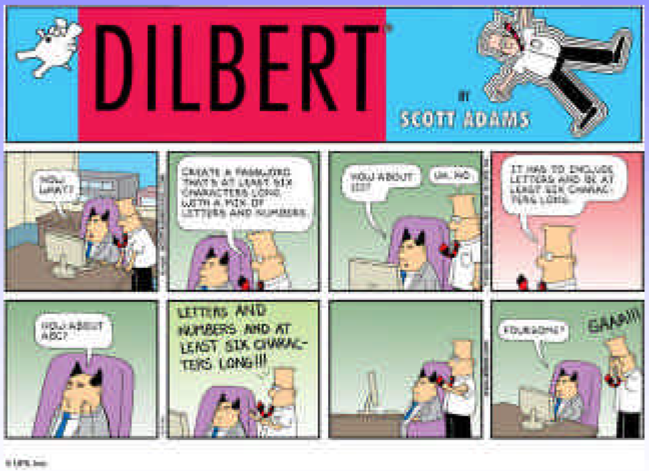
Physical Security (2)



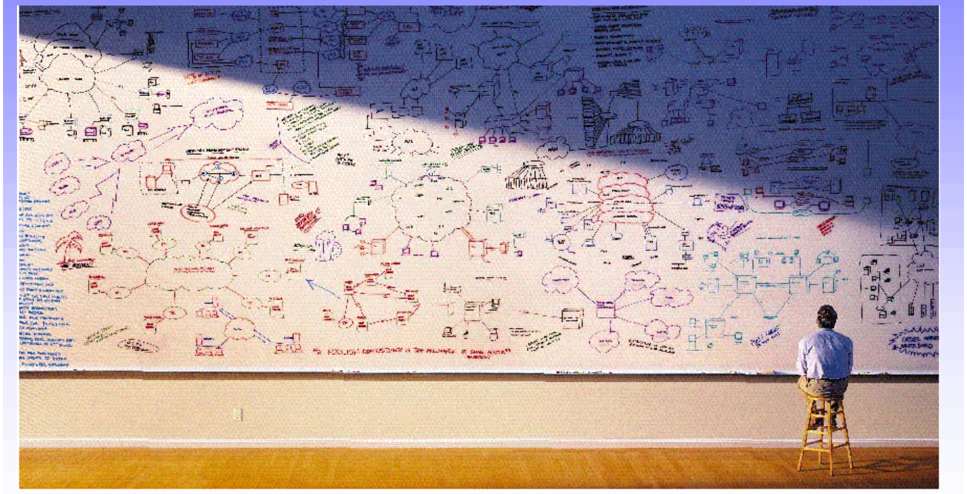


Operations Management

Access Control


DILBERT
BY
SCOTT ADAMS
NOW WHAT?
CREATE A PASSWORD THAT'S AT LEAST SIX CHARACTERS LONG WITH A MIX OF LETTERS AND NUMBERS.
HOW ABOUT 111?
UH, NO.
IT HAS TO INCLUDE LETTERS AND BE AT LEAST SIX CHARACTERS LONG.
HOW ABOUT ABC?
LETTERS AND NUMBERS AND AT LEAST SIX CHARAC-TERS LONG!!!
FOURSOME?
GAAA!!!
© UFS, Inc.

Systems development

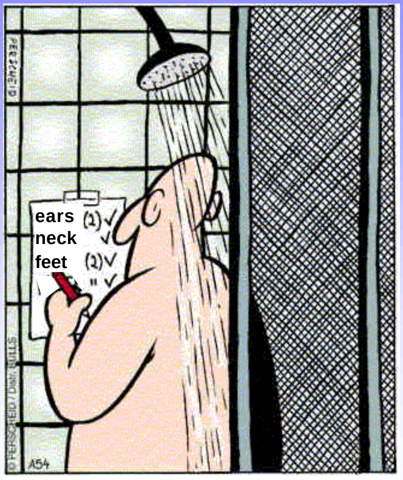


Information Security Incident Mgt.

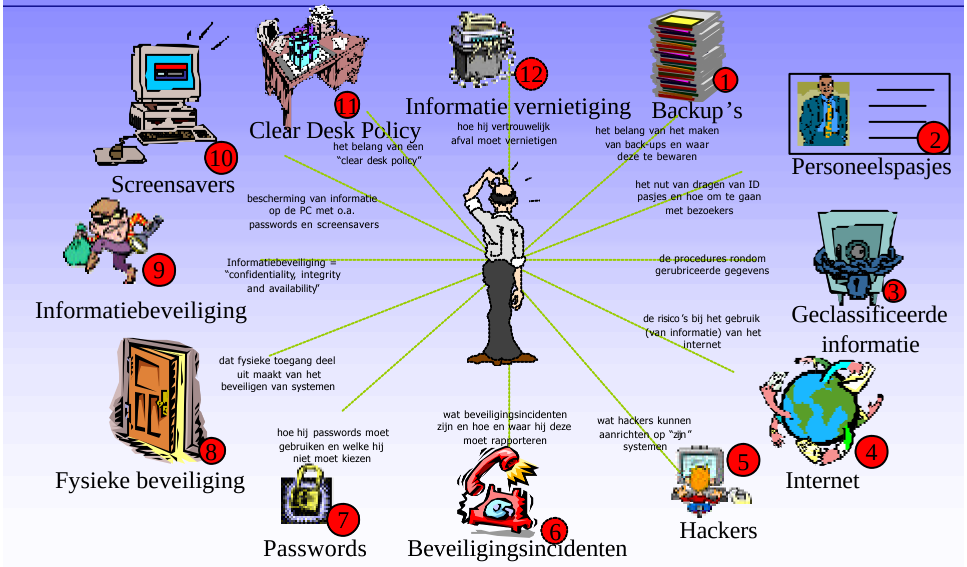
Business Continuity Management

Anybody here know how to play Microsofts' Flight Simulator ?
Quiek

Compliance



People



11 Clear Desk Policy

het belang van een "clear desk policy"

12 Informatie vernietiging

hoe hij vertrouwelijk afval moet vernietigen

1 Backup's

het belang van het maken van back-ups en waar deze te bewaren

2 Personeelspasjes

het nut van dragen van ID pasjes en hoe om te gaan met bezoekers

10 Screensavers

bescherming van informatie op de PC met o.a. passwords en screensavers

9 Informatiebeveiliging

Informatiebeveiliging = "confidentiality, integrity and availability"

3 Geclassificeerde informatie

de procedures rondom gerubriceerde gegevens

4 Internet

de risico's bij het gebruik (van informatie) van het internet

8 Fysieke beveiliging

dat fysieke toegang deel uit maakt van het beveiligen van systemen

7 Passwords

hoe hij passwords moet gebruiken en welke hij niet moet kiezen

6 Beveiligingsincidenten

wat beveiligingsincidenten zijn en hoe en waar hij deze moet rapporteren

5 Hackers

wat hackers kunnen aanrichten op "zijn" systemen

Top-20 security issues (1)

1. Risicomanagement
2. Screening medewerkers
3. Opleiding en bewustwording
4. Security Incident Management
5. Business Continuity Management
6. Handboek IB niet goedkeurd
7. Controleplannen (Compliance)
8. (Physical + Logical) Access Control (PPT)
9. patchmanagement
10. Inzicht in externe koppelingen

Top-20 security issues (2)

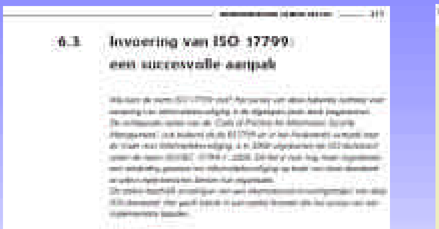
11. Protection of log information
12. Confidentiality agreements
13. Information classification guidelines
14. Change management
15. Mobile devices
16. Monitoring System Use
17. Management of Removable Media
18. OSG, TVE, OS Hardening
19. Clear Desk Policy
20. Asset management

Referenties

- Articles & presentations:
- ENISA ad hoc working group on risk assessment and risk management*, Inventory of risk assessment and risk management methods*
- GAO, *Information Security Risk Assessment: Learning from Leading Organizations* Books:
- NIST, *Sp800-30, Risk Management Guide for Information Technology Systems*
- ISO/IEC 27001; ISO/IEC 17799

- www.enisa.europa.eu
- www.gao.gov
- www.nist.gov
- www.iso.ch; www.nen.nl
- www.information-security-governance.com

Readings



6.3 Invoering van ISO 17799: een succesvolle aanpak

[illegible]

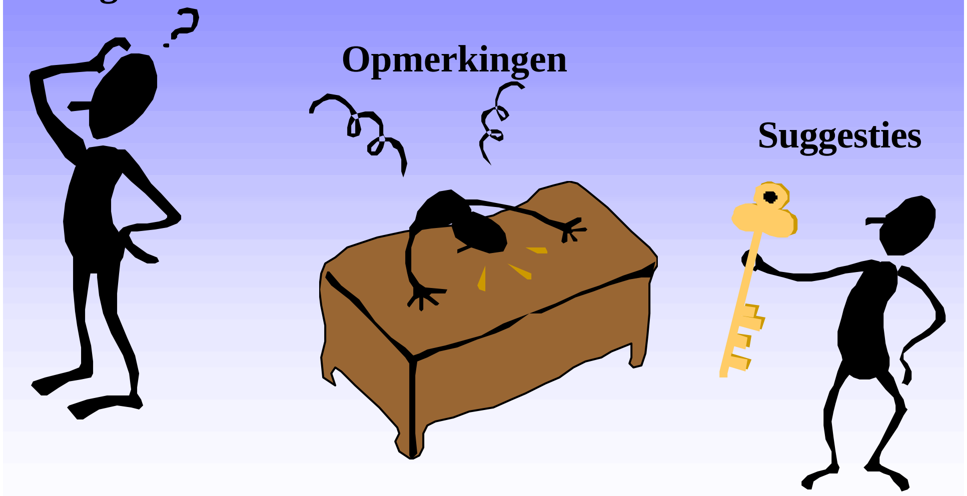
8.5 Information security governance

Casus bij financiële instellingen

[illegible]

Dank voor uw aandacht !

Vragen



Opmerkingen

Suggesties

Aart.Bitter@information-security-governance.com