Management requirements on IS

Eric Verheul
PricewaterhouseCoopers Advisory Security & Technology (S&T)
&
Radboud University Nijmegen
Security of Systems (SoS)

May 31, 2007
Agenda

• About PwC and RU
• Corporate governance and IT
• ISO 27001 and risk assessment
• Risk assessment in BS7799-3 standard
• ISO 27001 certification and outsourcing
• Dividing up information security
• Conclusion
Agenda

• **About PwC and RU**
• Corporate governance and IT
• ISO 27001 and risk assessment
• Risk assessment in BS7799-3 standard
• ISO 27001 certification and outsourcing
• Dividing up information security
• Conclusion
About PwC and RU

**PwC Security & Technology group**
- ISO 27001 implementation
- ISO 27001 certification
- Security audits/consultancy
- Privacy audits/consultancy
- Application penetration testing
- Identity management
- Cryptography/PKI

**RU Security of Systems group**
- Java program security (voting over the internet)
- Smart cards (Dutch biometric password)
- Penetration tests (War driving)
- Mathematical applications in information security (cryptography, quantitative risk assessments)
Agenda

• About PwC and RU
• Corporate governance and IT
• ISO 27001 and risk assessment
• Risk assessment in BS7799-3 standard
• ISO 27001 certification and outsourcing
• Dividing up information security
• Conclusion
SoX, Tabaksblat, COSO

• Corporate governance: the set of processes, customs, policies, laws and institutions affecting the way a corporation is directed, administered or controlled.
• Legal requirements in Sarbanes-Oxely (US) and Code Tabaksblat (NL)
• In 1992 COSO published its Internal Control—Integrated Framework often referred to as ‘COSO’
• COSO stands for “Committee of Sponsoring Organizations of the Treadway Commission”
• COSO deals with Enterprise Risk Management (ERM)
Example of Risks

Environmental Risks
- Capital Availability
- Regulatory, Political, and Legal
- Financial Markets and Shareholder Relations

Process Risks
- Operations Risk
- Empowerment Risk
- Information Processing / Technology Risk
- Integrity Risk
- Financial Risk

Information for Decision Making
- Operational Risk
- Financial Risk
- Strategic Risk
The ERM Framework

The eight components of the framework are interrelated ...

- Develop RA approach
- Perform RA
- Select/implement controls
Governance & IT

Enterprise Risk Management:
• is not about avoiding all risks, but
• is finding a right balance in taking risks and (future) profits/costs (‘risk-appetite’)

Enterprise Risk Management:
• relates to business processes
• is responsibility of management
• is based on risk assessments

Management should be in control of risks.
Governance & IT

- Corporate governance includes IT governance and includes Information Security.
- COBIT (Control Objectives for Information and related Technology) is an IT governance framework that closely aligns with COSO.
- COBIT is also based on ISO 27001.
Corporate governance and IT

CobiT

The CobiT framework - concept
Management’s IT expectations and IT responsibilities

Linking management’s IT expectations
With management’s IT responsibilities

What you get

Business Processes

What you need

IT Resources
- Data
- Application systems
- Technology
- Facilities
- People

Information

Information Criteria
- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

Do they match
Samas heeft weer last van IT-systeem

ANP

AMSTERDAM — Kantoorinrichter Samas rekent op een operationeel verlies in de tweede jaarhelft van het gebroken boekjaar. In de onderneming heeft vertraging opgelopen bij een project en dat kost haar geld. Dat liet Samas woensdag weten.

Het gaat om het automatiseringprogramma Harmony. De invoering ervan in Frankrijk kan pas over enkele maanden plaatsvinden. Kosten van dat project valen hoger uit dan verwacht. Met dit project gemoeide kostenbesparingen worden hierdoor pas in een later stadium zichtbaar, aldus Samas.

Als gevolg van de perielen met de automatisering lopen betalingen van klanten vertraging op. ‘Om die reden hebben we banken gevraagd om een verruiming van bestaande leningen. We hebben wat overbrugging nodig’, lichtte bestuursvoorzitter Hans van der Ven toe.

Door de gang van zaken voorziet Samas een operationeel verlies in de tweede jaarhelft van het boekjaar 2006-2007, dat eind maart afloopt. Wel denkt het bedrijf dat dit verlies lager is dan in de eerste helft van het jaar. Toen was er sprake van een verlies van €10,3 mln.

In de eerste jaarhelft leid Samas onder de streep een verlies van €11 mln. Het bedrijf heeft de laatste jaren flink gereorganiseerd. Het moest dat doen omdat de markt voor kantoorartikelen inzakte als gevolg van economisch slechte tijden.
Voorschrift Informatiebeveiliging Rijksdienst 1994 (VIR)

- Regulation on information security for Dutch central government (e.g. the departments).
- Short: 6 articles, 3 articles are the core.
- Introduces distinctive notion of dependency analyses: the extent governmental business processes are dependent on the security of information systems.

- **Places responsibility for information security at business process owner level (‘zorgplicht’).**
Business processes are tips of the iceberg
Practical risk assessment: issues and solutions

Business processes are tips of the iceberg

Fundamental questions:
• How to ensure that your risk assessment touches ‘everything’ sufficiently?
• How to ensure that you can compare various kinds of risks?
• How to ensure that management is really in control of risks?
Blind spots examples

June 2005:

**Citibank admits: we've lost the backup tape**

The retail finance division of Citigroup has admitted that a backup tape containing personal information on almost 4 million customers in the US has gone missing.

[...]

The United Parcel Service lost the tape on May 2nd, and it hasn't been seen since. The tape contains Social Security numbers and transaction histories on both open and closed accounts at the bank’s lending branches in the US.

[...]

The company admitted that it doesn't use encryption on its electronic transmissions, nor explained why it took so long to notify the public.
Corporate governance & Information Security

Corporate governance and IT is more than security.

Information Security:
• is just a part of corporate governance
• relates to business processes
• based on risk management/ risk assessments
• is a responsibility of management
• management should be in control of risks
  (…and not the IT department…)
Agenda

• About PwC and RU
• Corporate governance and IT
• **ISO 27001 and risk assessment**
• Risk assessment in BS7799-3 standard
• ISO 27001 certification and outsourcing
• Dividing up information security
• Conclusion
ISO 27001 and risk assessment

ISO 27001’s Information Security Management System

Risks to business processes (Business Risks)
Legal, regulatory, contractual (security) requirements

Information Security Management System

(Managed) Information security controls

ISO 17799: 2005
ISO 27001 and risk assessment

ISO 27001 (ISMS)

• Based on Plan-Do-Check-Act (PDCA) model

Figure 1 — PDCA model applied to ISMS processes
ISO 27001 (ISMS)

Plan-Do-Check-Act (PDCA) model:

**Plan**
- Develop risk assessment methodology
- Apply risk assessment and select controls from ISO 17799 (SoA)

**Do**
- Implement controls

**Check**
- Check and monitor controls

**Act**
- Maintain and improve the ISMS
ISO 27001 and risk assessment

ISO 17799:2005 (‘Controls’)

5 SECURITY POLICY
6 ORGANIZING INFORMATION SECURITY
7 ASSET MANAGEMENT
8 HUMAN RESOURCES SECURITY
9 PHYSICAL AND ENVIRONMENTAL 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

Description of controls is rather high-level.
Agenda

• About PwC and RU
• Corporate governance and IT
• ISO 27001 and risk assessment
• **Risk assessment in BS7799-3 standard**
• ISO 27001 certification and outsourcing
• Dividing up information security
• Conclusion
Risk assessment in BS7799-3 standard

ISMS

**Risk Assessment**

- Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.
- Develop criteria for accepting risks and identify the acceptable levels of risk.
- Should be suited to the ISMS, and the identified business information security, legal and regulatory requirements.

Key notions

- **Asset**: something of value for the organization
- **Legal or business requirements**
- **Value of an asset**: importance of asset to business (process).
- **Threat**: what can happen/achieved e.g., by an attacker (‘end result’) 
- **Vulnerability**: ‘usable’ weaknesses / scenarios 
- **Likelihood**: occurrence of threats and/or vulnerabilities
Risk assessment in BS7799-3 standard

ISMS

Assets
- Processes and Services
- Software
- Physical items
- People

Types of assets

- Information
  - The organization, its image and reputation and its business needs and requirements
  - People working in the organization and with the information
  - Services, media, IT and software that is used to store or process the information
ISMS

**Assets**
- Processes and Services
- Software
- Physical items
- People
Risk assessment in BS7799-3 standard

ISMS

Threats (examples)

- Earthquake
- Eavesdropping
- Environmental contamination (and other forms of natural or man-made disasters)
- Extremes of temperature and humidity
- Failure of communications services
- Failure of network components
- Failure of power supply
- Failure of water supply
- Fire
- Flooding
- Hrldware failure
- Hrricane

- Operational support staff error
- Power fluctuation
- Repudiation (e.g. of services, transactions, sending/receiving messages)
- Software failure
- Staff shortage
- Theft
- Traffic analysis
- Traffic overloading
- Transmission errors
- Unauthorized use of software
- Unauthorized use of storage media
- Use of network facilities in an unauthorized way
### Vulnerabilities (examples)

A.3.3 Computer and network Management (BS 7799 Part 1: Section 6)

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>The vulnerability could be exploited by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unprotected communication lines</td>
<td>eavesdropping</td>
</tr>
<tr>
<td>Poor joint cabling</td>
<td>communications infiltration</td>
</tr>
<tr>
<td>Lack of identification and authentication mechanisms</td>
<td>masquerading of user identity</td>
</tr>
<tr>
<td>Transfer of passwords in clear</td>
<td>network access by unauthorized users</td>
</tr>
<tr>
<td>Lack of proof of sending or receiving a message</td>
<td>repudiation</td>
</tr>
<tr>
<td>Dial-up lines</td>
<td>network access by unauthorized users</td>
</tr>
<tr>
<td>Unprotected sensitive traffic</td>
<td>eavesdropping</td>
</tr>
<tr>
<td>Single point of failure</td>
<td>failure of communications services</td>
</tr>
<tr>
<td>Inadequate network management</td>
<td>traffic overloading</td>
</tr>
<tr>
<td>Lack of care at disposal</td>
<td>theft</td>
</tr>
<tr>
<td>Uncontrolled copying</td>
<td>theft</td>
</tr>
<tr>
<td>Unprotected public network connections</td>
<td>use of software by unauthorized users</td>
</tr>
</tbody>
</table>
Risk Assessment / Treatment

1. Asset identification and ownership
2. Identification of legal and business requirements
3. Asset valuation
4. Identification and assessment of threats and vulnerabilities
   - For each asset
   - Implemented or projected controls
   - Identification of threats and vulnerabilities
   - Assessment of threats and vulnerabilities
   - Risk calculation
5. Risk treatment and management decision making
   → Risk Treatment plan
[6. Re-evaluate step 4.]
Asset valuation

### Risk assessment in BS7799-3 standard

<table>
<thead>
<tr>
<th>Risk</th>
<th>Criteria related to Confidentiality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Incorrectness of information can result in:</td>
</tr>
<tr>
<td></td>
<td>• fraud of less than Euro 2.500</td>
</tr>
<tr>
<td></td>
<td>• no bad publicity</td>
</tr>
<tr>
<td></td>
<td>• no damage to the operational management due to incorrect management decisions</td>
</tr>
<tr>
<td></td>
<td>• no risk for liability or non-compliance with rules and regulations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>Criteria related to Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>Incorrectness of information can result in:</td>
</tr>
<tr>
<td></td>
<td>• fraud of less than Euro 25.000</td>
</tr>
<tr>
<td></td>
<td>• bad publicity in local news media</td>
</tr>
<tr>
<td></td>
<td>• limited damage to the operational management due to incorrect management decisions</td>
</tr>
<tr>
<td></td>
<td>• limited risk for liability or non-compliance with rules and regulations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>Criteria related to Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Incorrectness of information can result in:</td>
</tr>
<tr>
<td></td>
<td>• fraud of substantially more than Euro 25.000</td>
</tr>
<tr>
<td></td>
<td>• bad publicity in national news media</td>
</tr>
<tr>
<td></td>
<td>• unacceptable damage to the operational management due to incorrect management decisions</td>
</tr>
<tr>
<td></td>
<td>• high risk for liability or non-compliance with rules and regulations</td>
</tr>
</tbody>
</table>
### SPRINT Business Impact Assessment

#### Confidentiality

<table>
<thead>
<tr>
<th>Business Consequences</th>
<th>Business Impact Rating</th>
<th>Explanatory comments</th>
</tr>
</thead>
</table>
| of unintended or unauthorised disclosure of information (worst case) | A: Business Survival Threatened  
B: Serious Damage  
C: Significant Damage  
D: Minor Impact  
E: Negligible | |

**C1** **COMPETITIVE DISADVANTAGE**  
How damaging would it be if information is disclosed to a competitor?  
| A | B | C | D | E |

**C2** **DIRECT LOSS OF BUSINESS**  
Could business be lost if information is disclosed?  
| A | B | C | D | E |

**C3** **PUBLIC CONFIDENCE**  
If information is disclosed, what damage | A | B | C | D | E |
Identification and assessment of threats and vulnerabilities

**BS7799-3**
- Provides many examples of threats and vulnerabilities for each ISO17799 chapter
- Provides some guidelines for the interpretation of threats and vulnerabilities and likelihood (Low, Medium, High), e.g.:

  *Low likelihood*
  It is not likely that the threat will occur, there are no incidents, statistics, motives, etc. that indicate that this is likely to happen.
## Identification and assessment of threats and vulnerabilities

### BS7799-3

#### Table C.6 Matrix with risk values

<table>
<thead>
<tr>
<th>Asset value</th>
<th>Level of threat</th>
<th>Level of vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>L</td>
<td>M</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>M</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>
Identification and assessment of threats and vulnerabilities

BS7799-3
• High complexity
Order ≈ #Assets X # Threats X # Vulnerabilities X # Controls
• Not enough practical guidance to ensure that all threats and vulnerabilities are properly addressed, i.e. to avoid ‘blind spots’.
• How can (bossiness-oriented) management ensure that all vulnerabilities, in particular those ‘deep-down’ the chain, are indeed adequately tackled?
Deep-down vulnerabilities: security in self developed software

```c
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
    // guaranteed to be random.
}
```
Risk assessment in BS7799-3 standard

Deep-down vulnerabilities: config ATMs
Deep-down vulnerabilities: PDF ‘protection’
Risk assessment in BS7799-3 standard

Deep-down vulnerabilities: Exchangeable Image File Format
Deep-down vulnerabilities: OWA

url = https://www.malicious.com
### Risk assessment in BS7799-3 standard

#### Deep-down Office macros/Office Clipboard

**Directory Listing for: /me/malicious/Office/word**

<table>
<thead>
<tr>
<th>Subdirectories:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>word_files/</td>
<td>Wed, 30 May 2007 13:05 CEST</td>
</tr>
</tbody>
</table>

**Files:**

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>infoWord.doc</td>
<td>75.4 KB</td>
<td>Wed, 24 Aug 2005 14:58 CEST</td>
</tr>
<tr>
<td>infoWord.doc.ppc</td>
<td>23.7 KB</td>
<td>Fri, 26 Aug 2005 17:30 CEST</td>
</tr>
<tr>
<td>infoWord.doc.ppg</td>
<td>17.9 KB</td>
<td>Fri, 26 Aug 2005 14:23 CEST</td>
</tr>
<tr>
<td>infoWord.doc.pw</td>
<td>16.0 KB</td>
<td>Fri, 26 Aug 2005 11:21 CEST</td>
</tr>
<tr>
<td>infoWord.rst</td>
<td>23.9 KB</td>
<td>Fri, 26 Aug 2005 17:30 CEST</td>
</tr>
<tr>
<td>infoWord.rst.pcs</td>
<td>16.0 KB</td>
<td>Fri, 26 Aug 2005 11:21 CEST</td>
</tr>
<tr>
<td>infoWord.zip</td>
<td>17.0 KB</td>
<td>Fri, 26 Aug 2005 14:20 CEST</td>
</tr>
<tr>
<td>infoEmc.pst.zip</td>
<td>17.1 KB</td>
<td>Fri, 26 Aug 2005 12:00 CEST</td>
</tr>
<tr>
<td>infoRunc.pst.zip</td>
<td>17.1 KB</td>
<td>Fri, 26 Aug 2005 11:19 CEST</td>
</tr>
<tr>
<td>word.htm</td>
<td>160.9 KB</td>
<td>Fri, 26 Aug 2005 12:54 CEST</td>
</tr>
</tbody>
</table>

**Tunnel Webb Server 0.24**
Enkele voorbeelden ‘uitbraak’ testen

Clipboard vulnerability MS internet explorer

Hi, I found an article in the *Kuwait Times* that I thought you might find interesting.

Kind Regards,
W.T.
Risk treatment and management decision making

**BS7799-3**

Decision-making:
- Knowingly accept the risk
- Reduce the risk
- Transfer of the risk
- Avoid the risk
- Residual risk
- Risk Treatment plan

Very important aspect of IT security, but BS7799-3 provides only little practical guidance, e.g. on:
- Comparison and relation of risks in different business processes
- Effective control selection including cost of controls
- Do you really want to bother (business-oriented) management with firewall selection?
Summary on BS7799-3

• High Complexity:
  Order ≈ #Assets X # Threats X # Vulnerabilities X # Controls
• Difficulty in getting all (real) threats and vulnerabilities visible
• Little practical guidance on effective control selection

• Difficult for management to be really in control.
• Risk of becoming paper tiger, forgetting the real threats and vulnerabilities deep-down the chain.
Agenda

• About PwC and RU
• Corporate governance and IT
• ISO 27001 and risk assessment
• Risk assessment in BS7799-3 standard
• **ISO 27001 certification and outsourcing**
• Dividing up information security
• Conclusion
NL-Certification

ECP.NL (27001 scheme)

Raad voor Accreditatie (Accreditation Body)

Certification Bodies
- Ernst & Young, Kema, BSI
- TÜV, DNV
- PricewaterhouseCoopers

Centraal College van Deskundigen

Assesses and Awards certificates

Organization ISMS
ISO 27001 and IT outsourcing

Issue in certification against ISO 27001:
• how to deal with an organization that has outsourced its IT?
• what kind of agreements (SLAs) on information security are required?
ISO 27001 and IT outsourcing

1. ‘Specification’ of security requirements, e.g.:
   • Identification of legal and business requirements
   • A threat analysis
   • Value of the information and/or assets
   • Indications of ISO 17799 controls required
2. A (partial) risk analysis within the scope of the organisation itself → A (substantiated) selection of ISO 17799 controls.

4. IT outsourcer is provided with 1. and performs (partial) risk analysis within their scope → A (substantiated) selection of ISO 17799 controls.
5. Organisation needs to validate or let validate analysis.
6. IT outsourcer implements ‘own’ ISO 17799 controls
7. IT outsourcer provides assurance that controls are indeed suitable implemented (e.g. using a third party auditor).
8. IT outsourcer periodically reports on the performance of these controls, including any security incidents that occurred.
ISO 27001 and IT outsourcing

Advantage:
- Less complex (e.g., less assets to consider by the organization, no specialized IT vulnerabilities to consider) \(\rightarrow\) more focused
- Everybody is doing what they are good at
- Better manageable
Agenda

• About PwC and RU
• Corporate governance and IT
• ISO 27001 and risk assessment
• Risk assessment in BS7799-3 standard
• ISO 27001 certification
• **Dividing up information security**
• Conclusion
Why don’t treat other departments / business processes in organization as ‘external’ outsourcer?
### Dividing up information security

1. ‘Specification’ of security requirements, e.g.:
   - Identification of legal and business requirements
   - A threat analysis
   - Value of the information and/or assets
   - Indications of ISO 17799 controls required

2. A (partial) risk analysis within the business process scope → (substantiated) selection of ISO 17799 controls.


4. Business process determines the supporting business processes or clusters (SBPs) that are security relevant.

5. SBPs are provided with 1. and performs (partial) risk analysis within their scope → (substantiated) selection of ISO 17799 controls.

6. BP needs to validate or let validate analysis.

7. SBPs implement ‘own’ ISO 17799 controls

8. SBPs provide assurance that controls are indeed suitable implemented (e.g. using a third party auditor).

9. SBPs periodically report on the performance of these controls, including any security incidents that occurred.
Dividing up information security

- HR
- Third parties
- Housing
- Logistics
- Facilities
- Training Department
- Finance Department
- Audit department
- IT Development
- Network management
- Database management
- Internet Service Providers
- Servers
- Applications
- Hardware Suppliers
Dividing up information security

Advantage:
• Less complex (e.g., less assets to consider by the business process, no specialized IT vulnerabilities to consider) → more focused
• Everybody is doing what they are good at
• Better manageable by business process owner
Agenda

- About PwC and RU
- Corporate governance and IT
- ISO 27001 and risk assessment
- Risk assessment in BS7799-3 standard
- ISO 27001 certification and outsourcing
- Dividing up information security
- Conclusion
Conclusion
Thank you!