ENISA Workshop on Risk Management

# Risk Management in the information security consulting sector

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

October 13, 2006


PRICEWATERHOUSECOOPERS

# Agenda

- About PwC and RU
- ISO 27001 and risk assessment
- Practical risk assessment: issues and solutions

# Agenda

- About PwC and RU
- ISO 27001 and risk assessment
- Practical risk assessment: issues and solutions

# 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

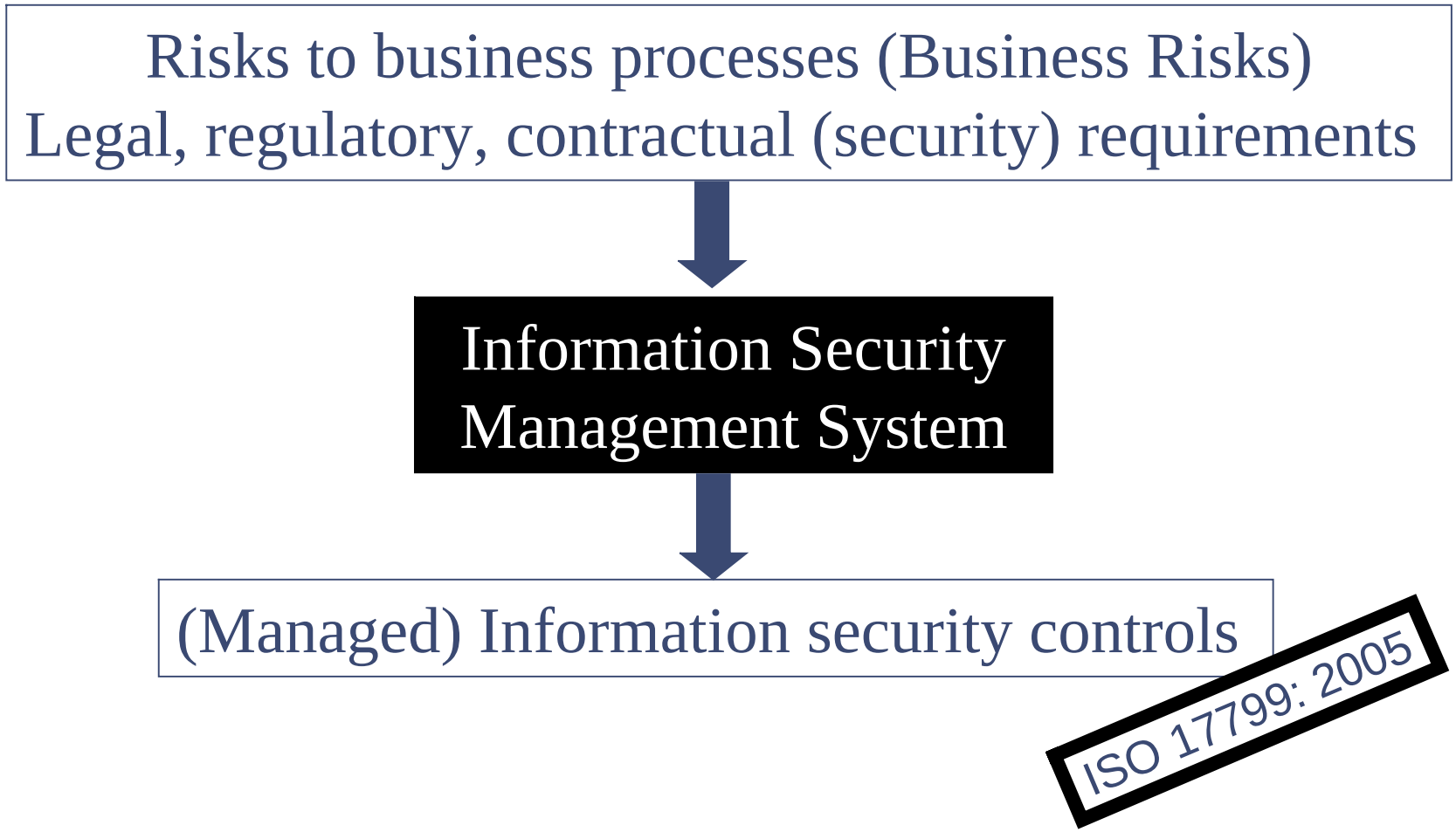
## RU Security of Systems group

- 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
- ISO 27001 and risk assessment
- Practical risk assessment: issues and solutions

# ISO 27001's Information Security Management System



# ISMS and risk assessment (clauses 4.2.1 c) – j) )

- Define the risk assessment approach of the organization
- Identify the risks
  - identify assets
  - identify threats to assets
  - identify vulnerabilities / impacts
- Analyze and evaluate the risks
- Identify and evaluate options for the treatment of risks
- Select control objectives and controls for the treatment of risks
- Obtain management approval of the proposed residual risks
- Obtain management authorization to implement and operate the ISMS
- Prepare a Statement of Applicability (SoA)

# ISMS and risk assessment (clauses 4.2.1 c)

- Define the risk assessment approach
- Identify the risks
  - identify assets
  - identify threats to assets
  - identify vulnerabilities
- Analyse and evaluate
- Identify and evaluate treatment of risks
- Select controls for the treatment of risks
- Obtain approval of the proposed residual risks
- Authorization to implement and operate the ISMS
- Statement of Applicability (SoA)

Simple theory, but not easy to implement in practice adequately, i.e. without leaving any '**blind spots**'.

# 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.**

# Blind spots examples

# Agenda

- About PwC and RU
- ISO 27001 and risk assessment
- Practical risk assessment: issues and solutions

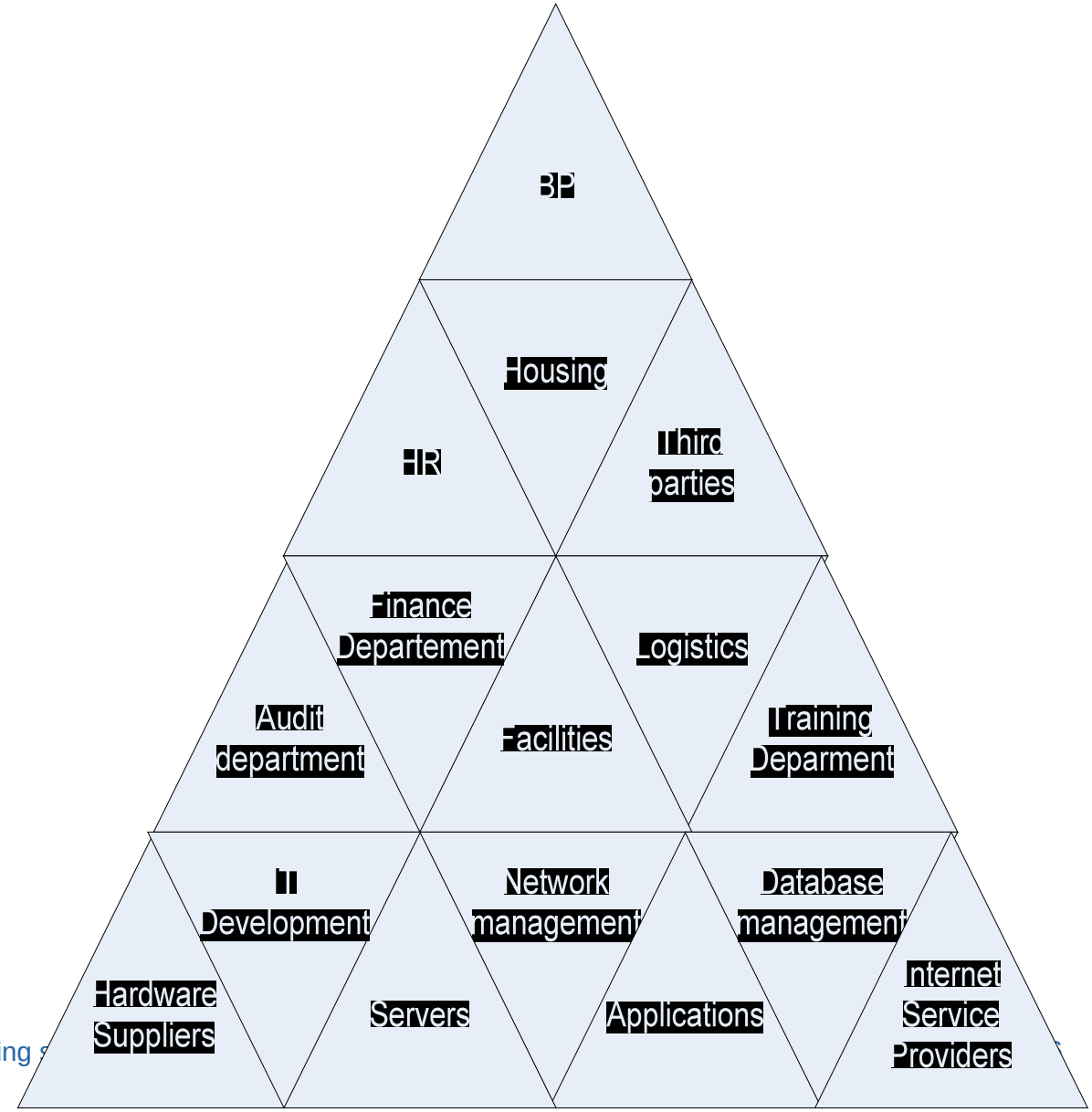
# Information security at business processes

| Risk | Criteria related to *Integrity* |
|---|---|
| *Low* | Incorrectness of information can result in:<br>•fraud of less than Euro 2.500<br>•no bad publicity<br>•no damage to the operational management due to incorrect management decisions<br>•no risk for liability or non-compliance with rules and regulations |
| *Medium* | Incorrectness of information can result in:<br>•fraud of less than Euro 25.000<br>•bad publicity in local news media<br>•limited damage to the operational management due to incorrect management decisions<br>•limited risk for liability or non-compliance with rules and regulations |
| *High* | Incorrectness of information can result in:<br>•fraud of substantially more than Euro 25.000<br>•bad publicity in national news media<br>•unacceptable damage to the operational management due to incorrect management decisions<br>•high risk for liability or non-compliance with rules and regulations |

Risk Criteria related to *Availability*

Risk Criteria related to *Confidentiality*

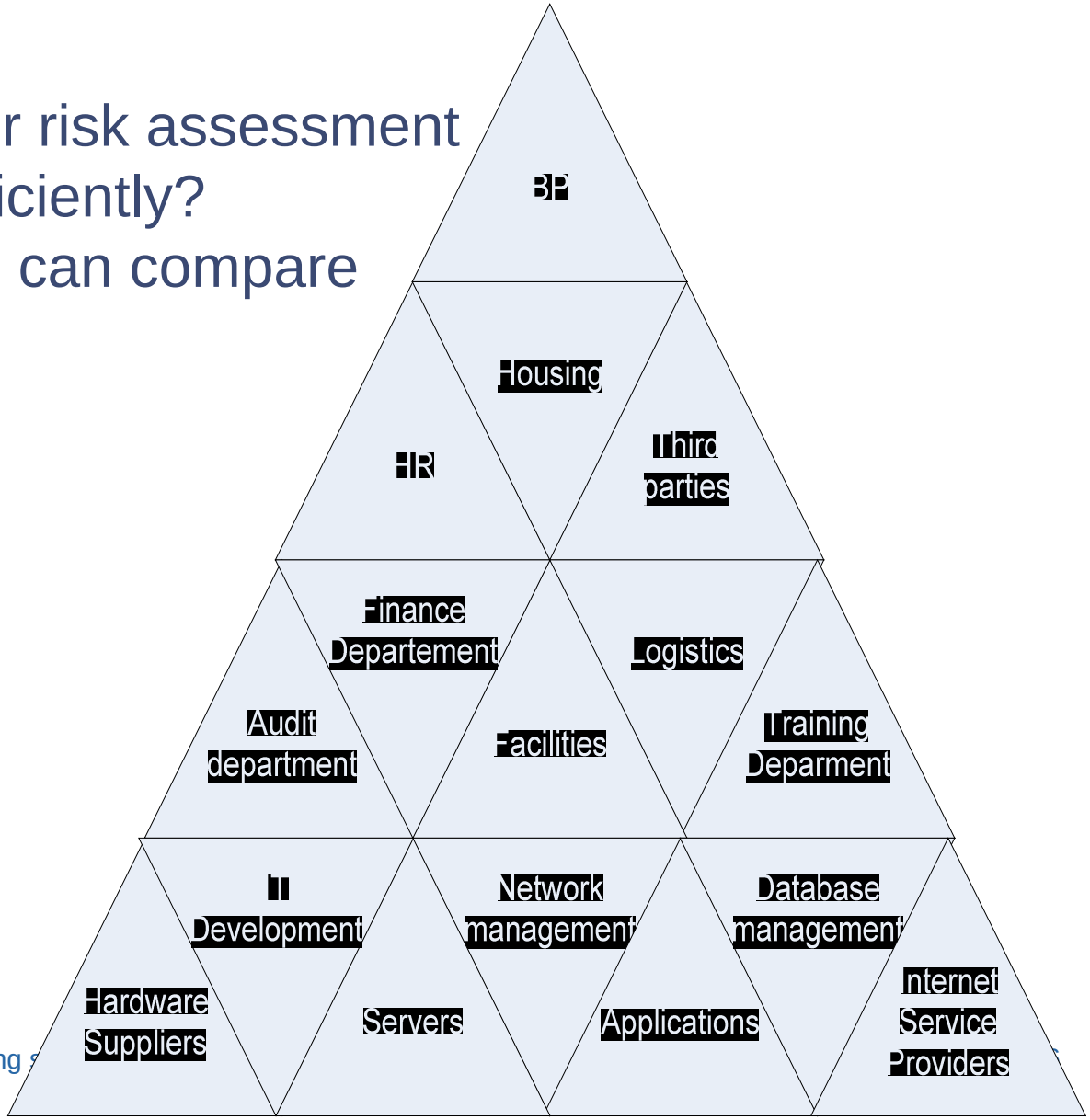
# Business processes are tips of the iceberg



# 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?



# Solutions

Direction of solution:

- consistent quantitative risk assessment methodologies throughout all ‘chains’
- it seems that the ENISA roadmap classifies this only as a ‘medium term priority’

# Thank you!