RAIFFEISEN INFORMATIK

How to set up a CSIRT in an ITIL driven organization

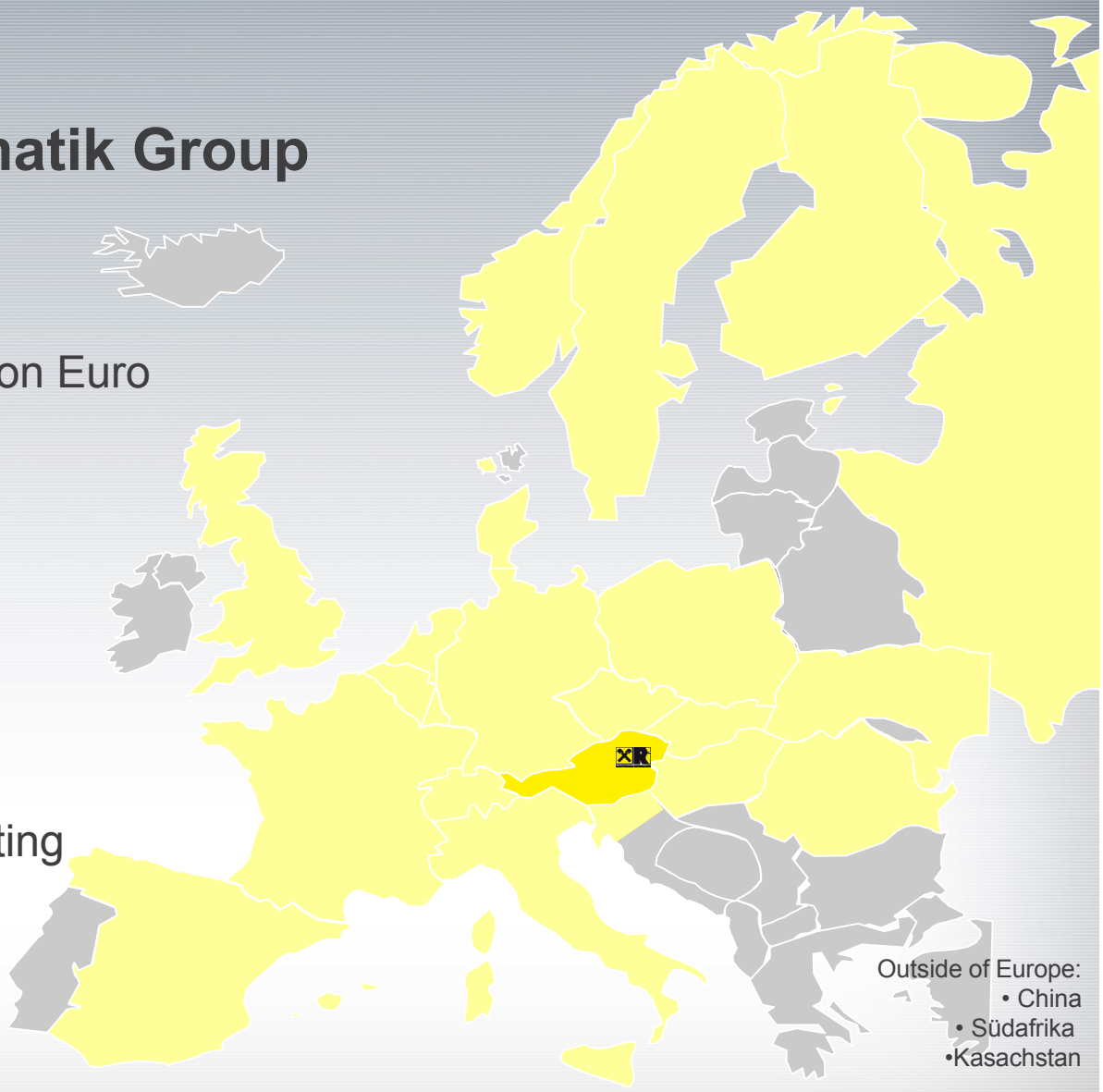
Christian Proschinger
Raiffeisen Informatik GmbH

- Introduction R-IT CERT
- Idea
- Introduction to ITIL
- Example Vulnerability Management
- Lessons Learned

Raiffeisen Informatik Group

27 Locations
3,000 Employees
Turnover 2009: 1.2 Billion Euro
40 years experience

IT Services
- IT Operations
- Outsourcing
- Security Services
- Client Management
- IT & Software Consulting
- Output Services



Outside of Europe:
• China
• Südafrika
•Kasachstan

RAIFFEISEN INFORMATIK

Security Competences at Raiffeisen Informatik

- **Department Information Security Management**
  - Information Security Management System
  - ISO 27001
  - Focus on Risk Management
- **Department Security Competence Center**
  - Founded 2005
  - Headquarter of Raiffeisen Informatik CERT Austria
  - Penetration Testing
- **Responsible person/team for each Business Service as well as for each Technical Component**

General Situation

- **Large scale IT organization have to be standardized and to be compliant**
  - IT Infrastructure Library
  - Business process maps
  - ISO 27001
  - COBIT
- **CSIRT**
  - Customized services for constituency
  - Guidelines
    - helpful but generic

General Situation

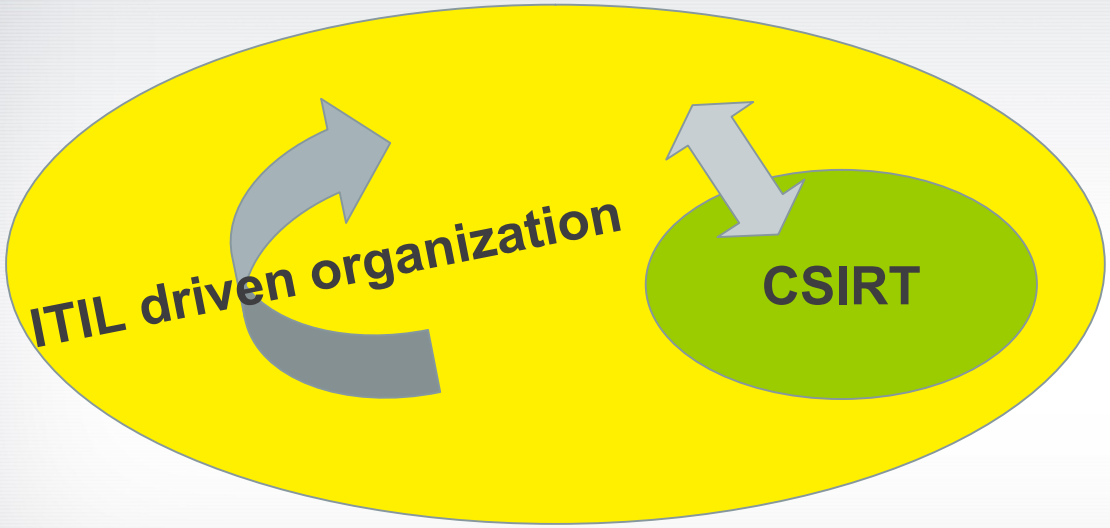
- **IT Infrastructure Library**
  - Best practice library
  - De-facto standard

  - 76 % of organizations align IT Service Management to ITIL*
  - Popular processes
    - Incident Management
      - Service Desk
      - Incident Management Process
    - Problem Management
    - Information Security Management

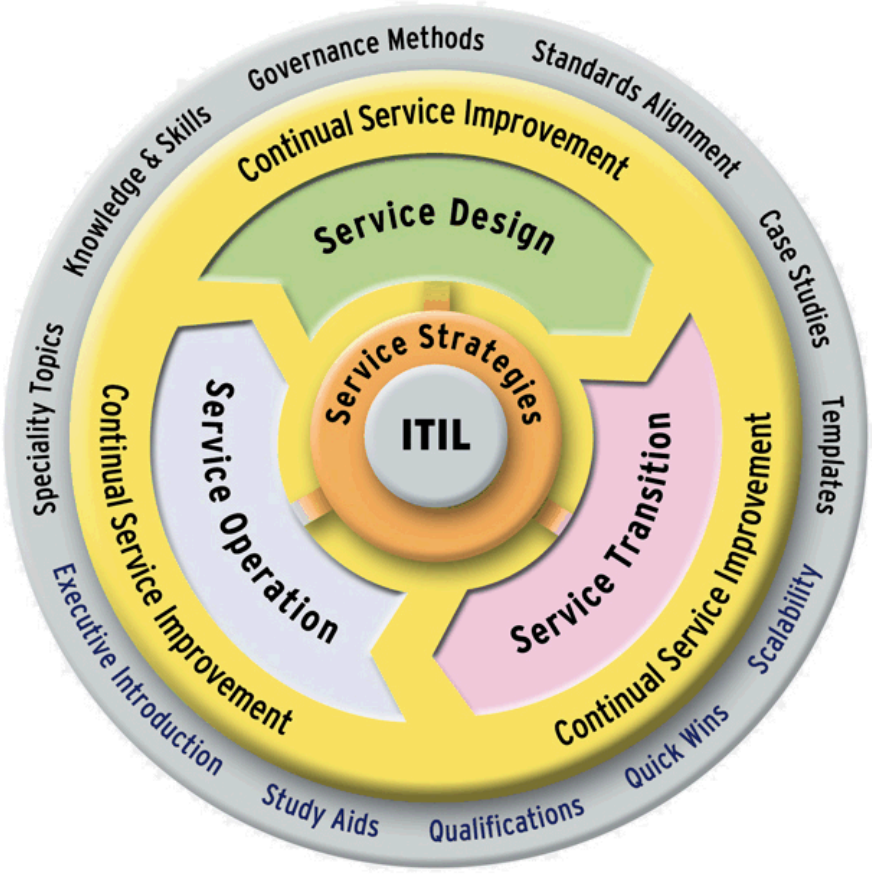
*IT Service Management Studie MATERNA

Questions

- **What are the implications of ITIL concerning**
  - setting up a CSIRT
  - operate a CSIRT



Introduction to IT Infrastructure Library



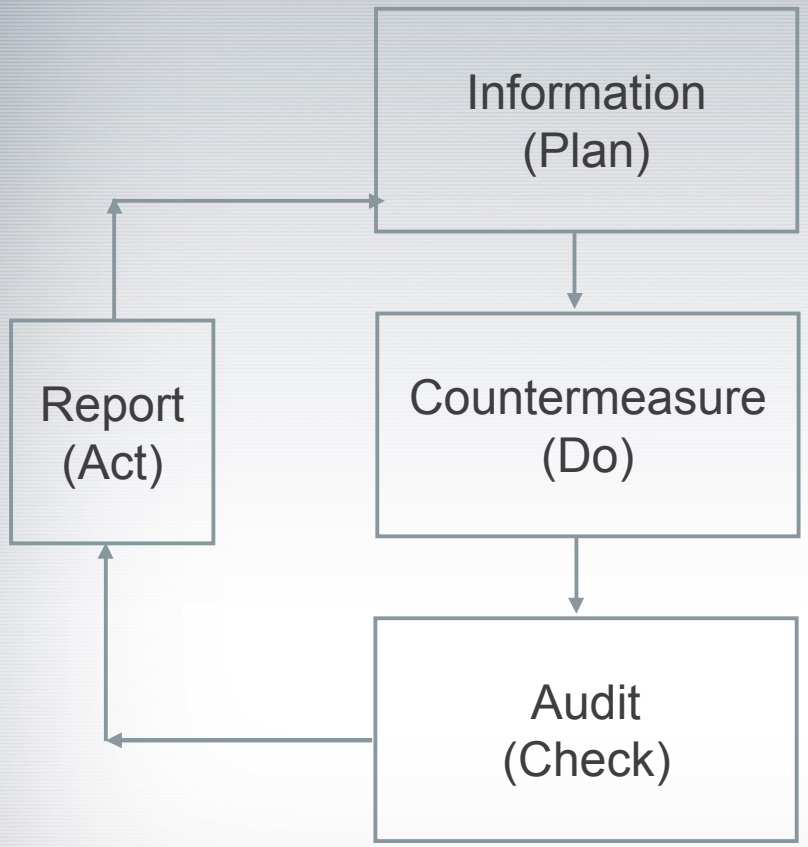
- **5 Core publications**
  - Service strategy
  - Service design
  - Service transition
  - Service operation
  - Continual service improvement
- **Target is an IT alignment to business processes**

Source: ITIL v3 The official Introduction to the Service Lifecycle: TSO (OGC); 2007

Service Strategy

Service Strategy	Service Design	Transition	IT Operations	Service Improvement
▪ Strategy development ▪ Service Portfolio Management ▪ Financial Management ▪ Demand Management	Management of: ▪ Service Catalog ▪ Service Level ▪ Capacity ▪ Availability ▪ IT Service Continuity ▪ Information Security ▪ Supplier	▪ Planning and Support ▪ Service Asset and Configuration Mgmt ▪ Chance Mgmt ▪ Release and Deployment Mgmt ▪ Service Validation & Testing Evaluation ▪ Knowledge Mgmt	▪ Event Management ▪ Incident Management ▪ Problem Management ▪ Request Fulfillment ▪ Access Management	Service Reporting ▪ 7-Step Improvement process ▪ quality improvement ▪ Service Measurement

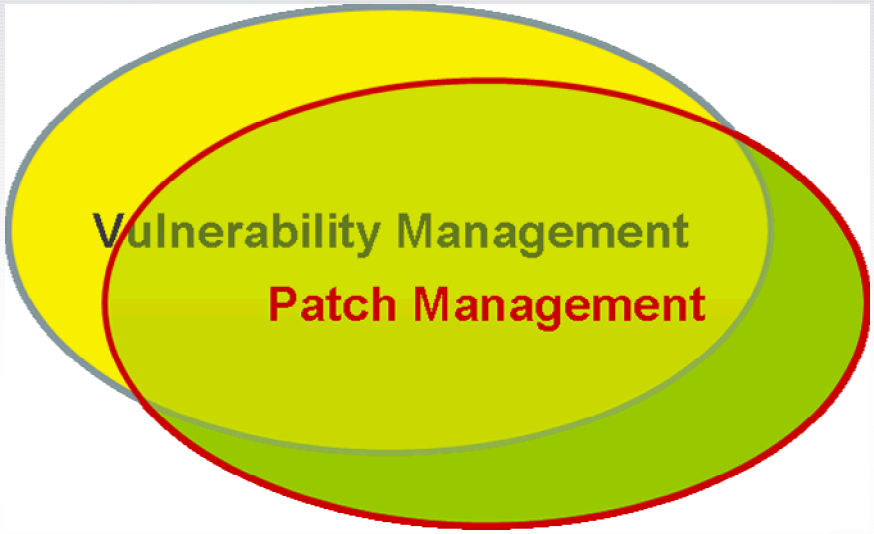
Example Vulnerability Management



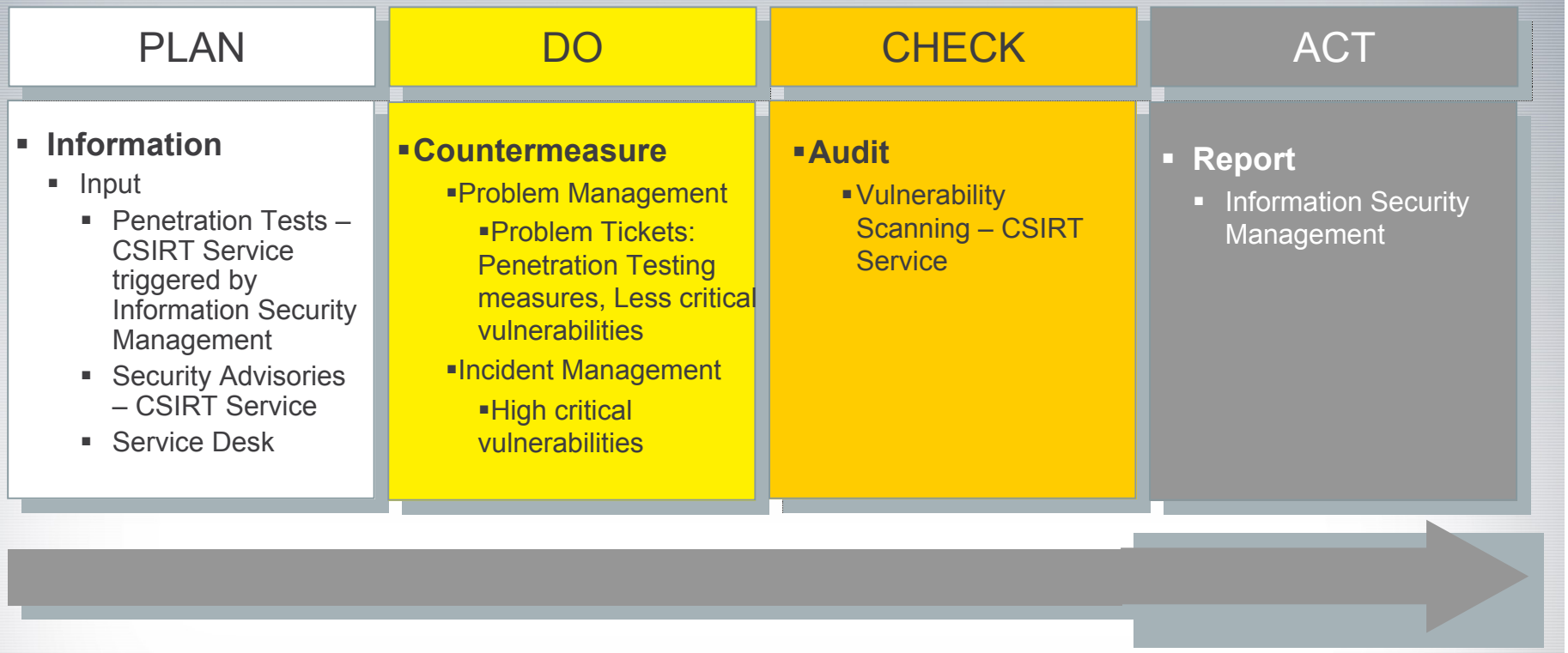
- **Information Security Management Process**
  - ISO 27001:2005
  - Deming Cycle (Plan-Do-Check-Act)
- **CSIRT can produce added value**
  - Economies of scale
  - Quality

Example Vulnerability Management

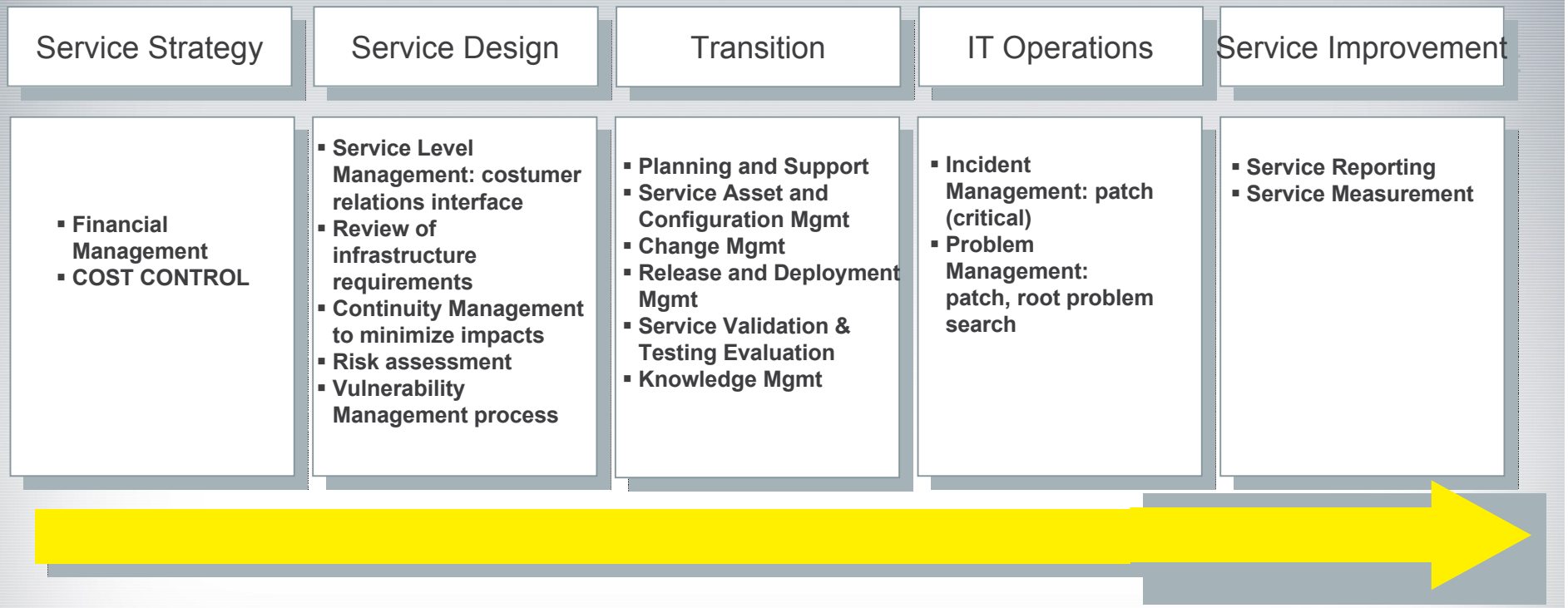
- **Vulnerability Management != Patch Management ➔ TRUE**
  - Workarounds
  - Configuration issues
  - Design issues
  - Functional patches



Example Vulnerability Management



Patch Management: affected ITIL Processes



RAIFFEISEN INFORMATIK

Lessons Learned

- **Vulnerability Management != Patch Management**
- **Incident != Security Incident**
- **Service Strategy**
  - Utility
  - Warranty ➔ USP Constituency
- **Service Design**
  - Information Security Management
    - ISO 27001:2005 good preparation for FIRST accreditation (Site Visit)
    - Information Security Management System
    - Define clear „interfaces“
    - Use the experience of your ISM Team
    - Easy way to achieve “separation of duties”
- **Service Operation**
  - Incident Management: Service Desk
    - Process can be easily adopted for security incident management
  - Problem Management: Good way to implement penetration test measures

Summary

- **Considering ITIL offers advantages**
- **Important processes**
  - Incident Management
  - Problem Management
  - Information Security Management
    - ISO 27001:2005 provides a good basis
- Maybe a possibility to set up the process of CSIRTs easier

Thank you for your attention!

Raiffeisen Informatik GmbH
Lilienbrunngasse 7-9
A-1020 Wien

T +43 1/99 3 99 - 0
F +43 1/99 3 99 - 1100
E info@r-it.at

www.raiffeiseninformatik.at