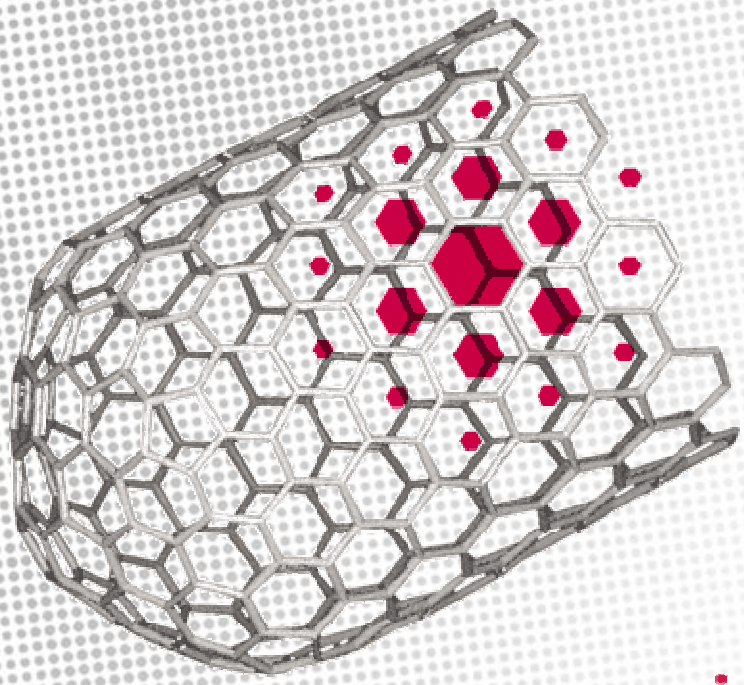


RAPID and ISO 27001

SASG meeting

Februari 2009

Auke van Balen

FEI COMPANY™

TOOLS FOR NANOTECH

Content of this presentation

- What is RAPID?
- Security questions
- How does RAPID look like
- Certification: up for ISO 27001
- Where is FEI on certification?
- Questions

Examples of FEI instruments

Remote Access Program for Interactive Diagnostics

Why RAPID?

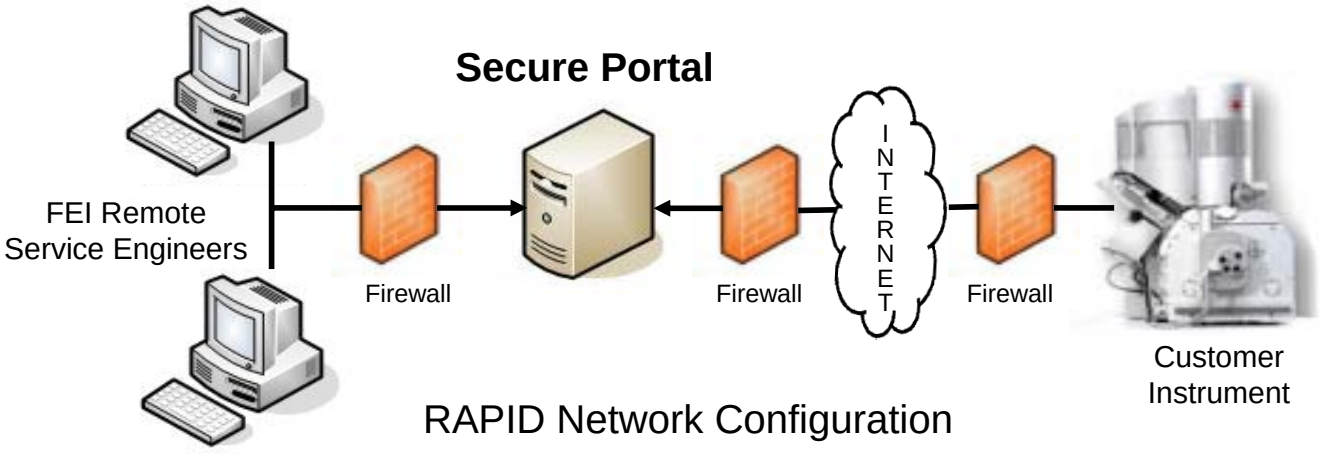
- Improve service response time
- Application assistance
- Possibility for data mining and collecting usage statistics
- Reduce workload and travel for service engineers
- Some places are difficult to get to: KAUST in Saudia Arabia

RAPID
REMOTE DIAGNOSTICS

Security questions

- How to get to the customer's instrument
- Getting permissions from corporate IT
- Who can do what:
  - Role Based Access Control
  - My Engineers
- Why should I trust FEI?
  - Certification
- BBWY: customer initiates connection (and can disconnect when suspicious)

RAPID Network setup



RAPID Network Configuration

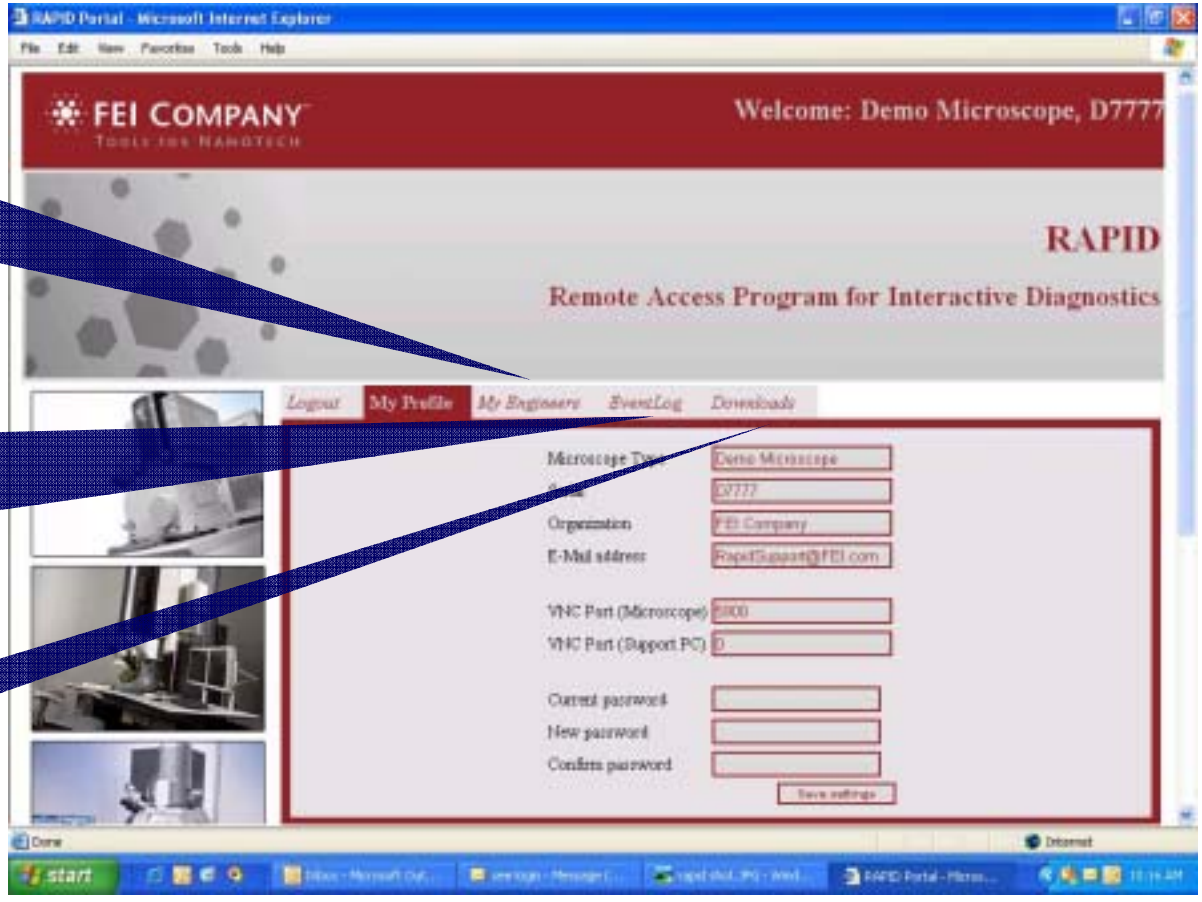
- Outbound connnections are generally OK
- IT needs to be involved: bandwidth consumption
- Servers at different locations in the world for optimum connection performance and redundancy

Initiating a RAPID Session…

With the My Engineers feature, manage users… enable and disable access

View “Event Log” to see history of RAPID sessions, including who has accessed your system.

Download software updates with file transfer feature

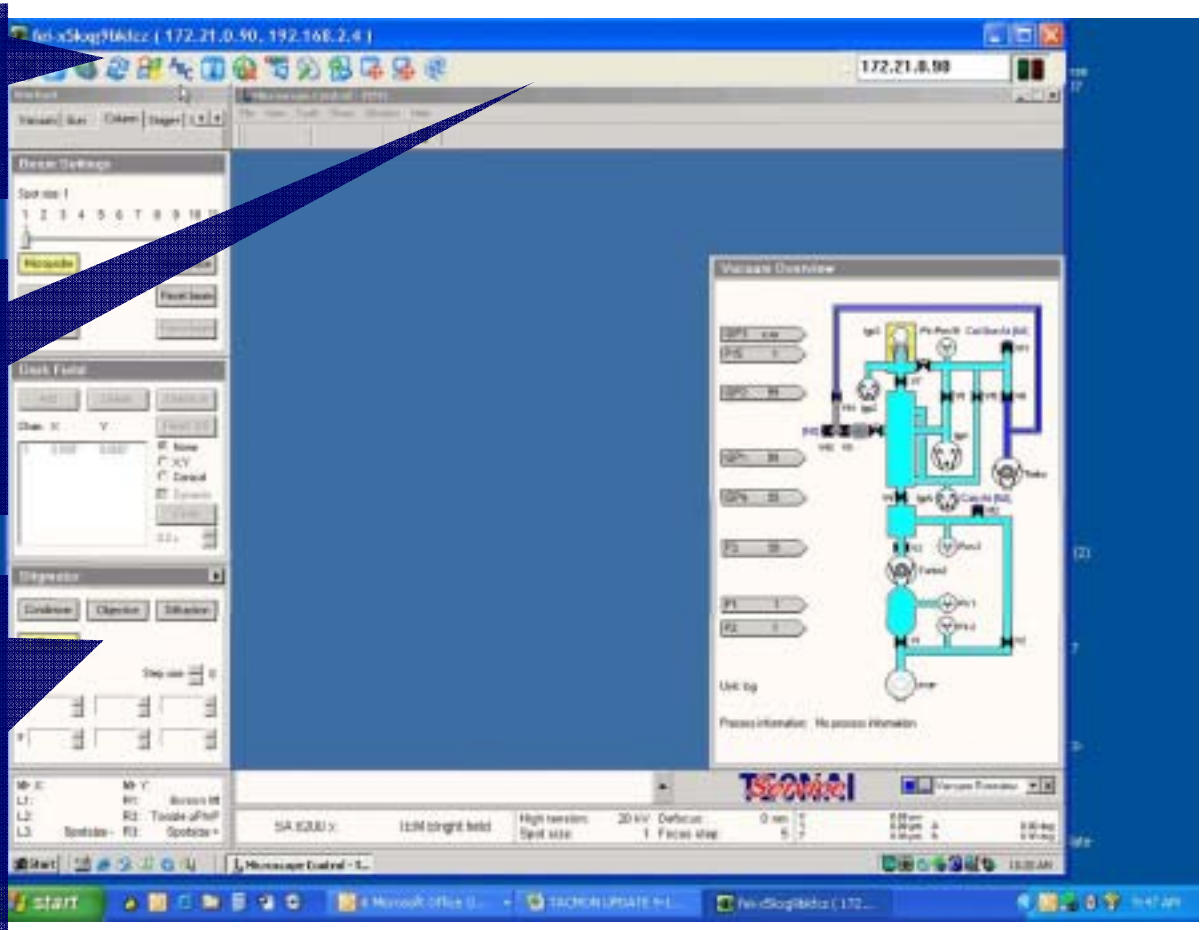


Using RAPID…

Tech Support Engineer "sees" what you see… in real-time.

Live chat with FEI's TSE or FSE to effectively explain your system concerns.

RSE runs diagnostics routines, views configurations uploads log files and modifies settings for optimum performance



Security lessons learned

- RAPID is accepted by most customers except those with very stringent security requirements (defense industry, IBM, Intel, Samsung, …)
- Accountability/traceability essential
- Independent security review by Cap Gemini was a great help
- Hacktest did not show weaknesses

ISO 27001: Code for information security

- Why certification?
  - Independent judgement of the security measures
  - Learning exercise for the organization
- Compliancy to ISO 27001 is expected to be standard practice, just as for ISO 9000 or ISO 14001

ISO 27001: two standards

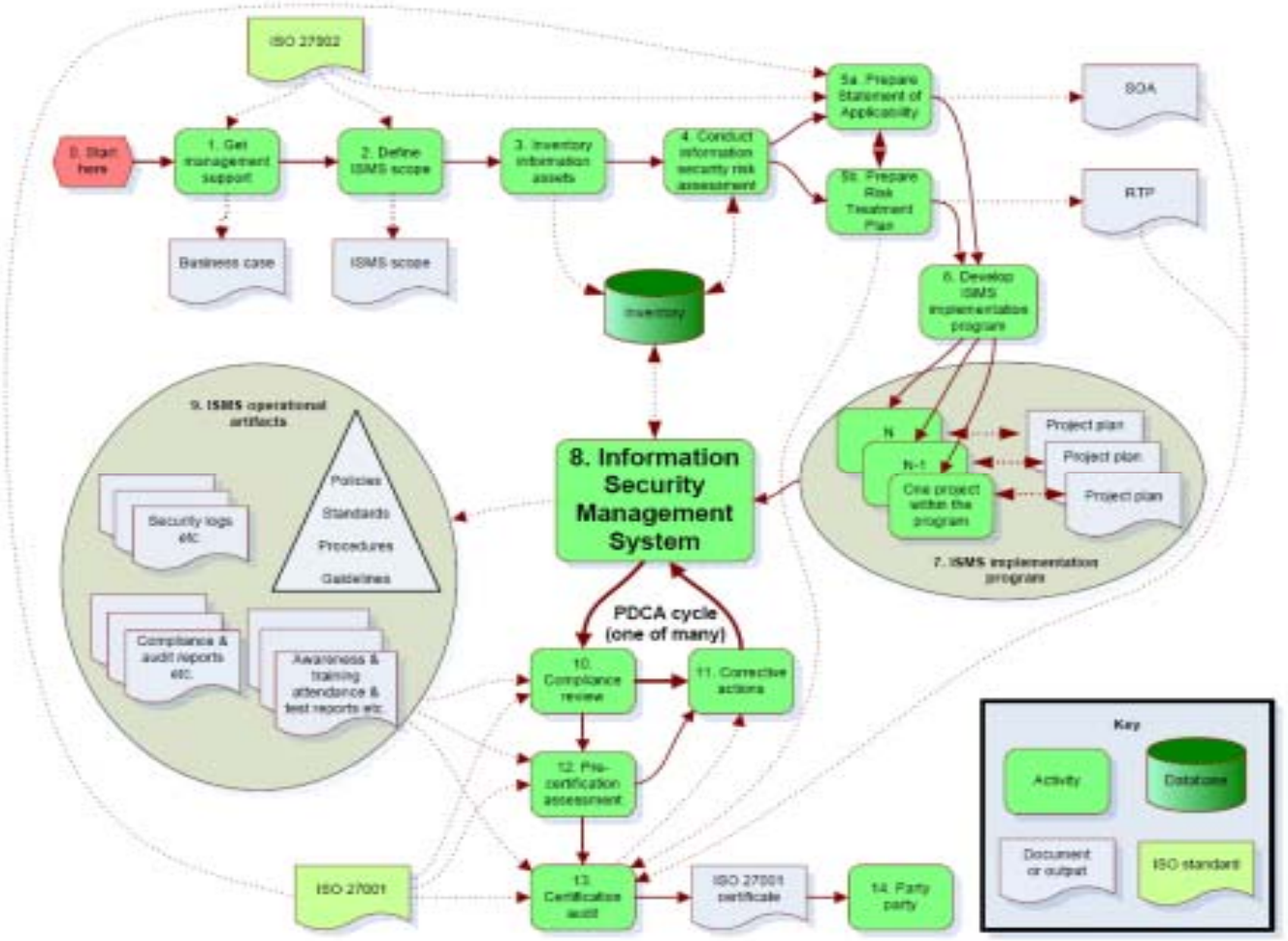
- ISO 27001
  - General description of information security
  - Security measures description: 120 measures
- ISO 27002
  - Part 1: the security measures formulated as norm: “shall”
  - Part 2: Information Security Management System
    - Plan-do-check-action cycle

Certification for ISO 27001 (1)

There are 6 steps in the process of getting certified:

1. **Define Scope & boundaries**
2. **Create Policy statement**
3. **Risk Assessment - Identify Threats**
4. **Risk Assessment - Manage the identified Risks**
5. **Select & Implement, Controls & Objectives for risk mitigation**
6. **Prepare Statement of Applicability**

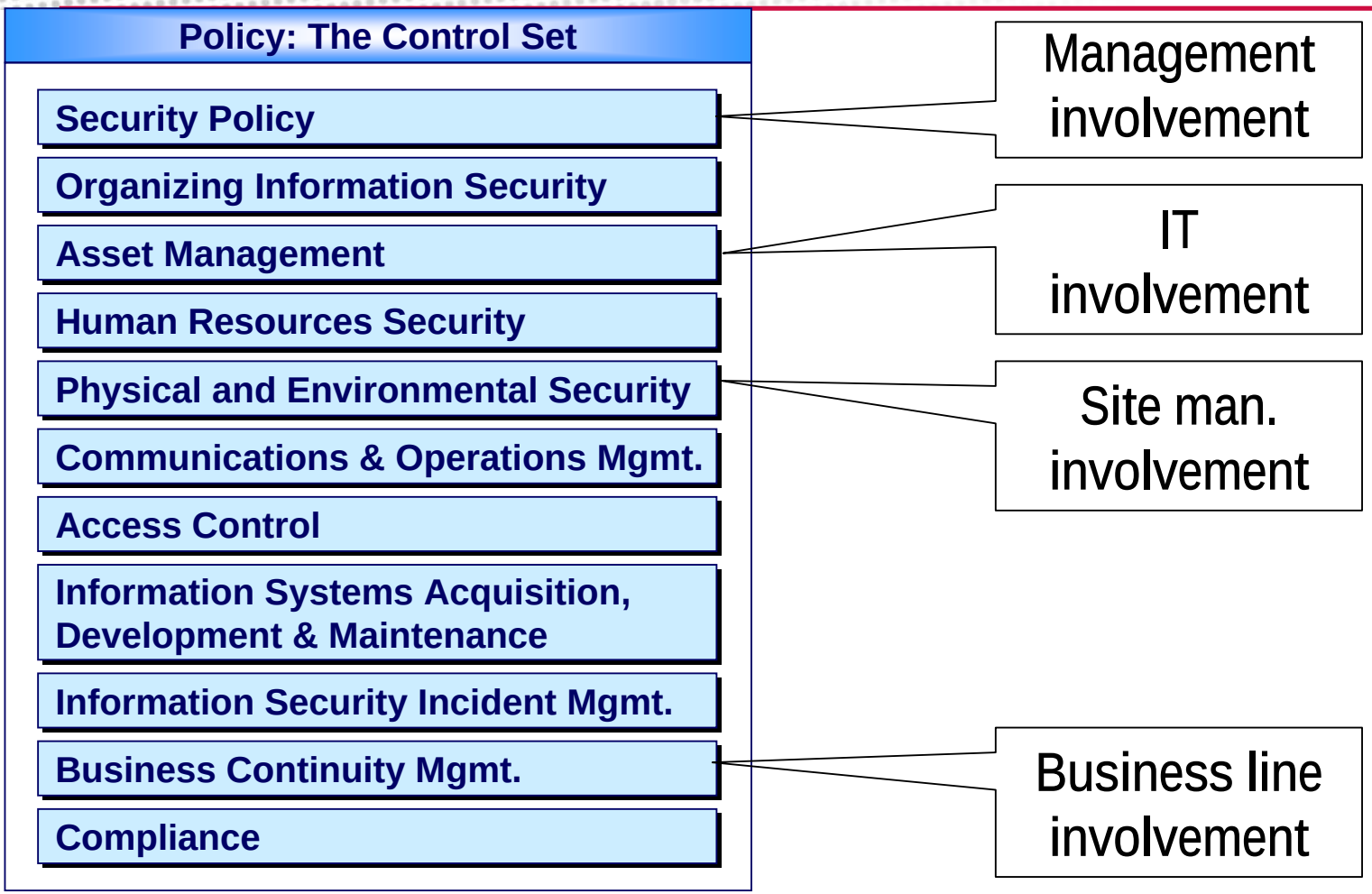
Certification for ISO 27001 (2)



Risk assesement

- Not all of the 120 measures are applicable in your organisation
- Make an analysis of each measure and estimate the impact: Impact = probability * damage
- Make quantitive: express in $$. frequency,…
- Methods like CRAMM (Central Risk Analysis and Management Method) are strongly recommended

Ingredients



Where is FEI with the certification?

- Cap Gemini as security consultants
- Risk Analysis completed
- Information Security Management System: documentation complete, in review
- Management awareness: first presentations given, growing but not entirely there yet
- Positive feedback from organisation
- Certification completed: begin 2010

Conclusions

- RAPID has proven to have value for customers
  - More than 500 customers accepted so far
- Security model accepted
- On our way to be ISO 27001 certified, will take some time

Questions?