Information Security Management

Dipl.-Ing. (FH) Frank Wagner

Agenda

- Importance of Information Security
  (IT-Security vs. Information Security)
- Information Security Policy
- Information Security Organization
- Information Security Awareness
- Information Security Audits
- Information Security Risk Management

Corporate structure 2007

Merck Group

Business sectors

Divisions

Pharmaceuticals	Chemicals
Merck Serono*	Liquid Crystals
Generics**	Performance & Life Science Chemicals
Consumer Health Care	

Cross-divisonal functions / Central functions

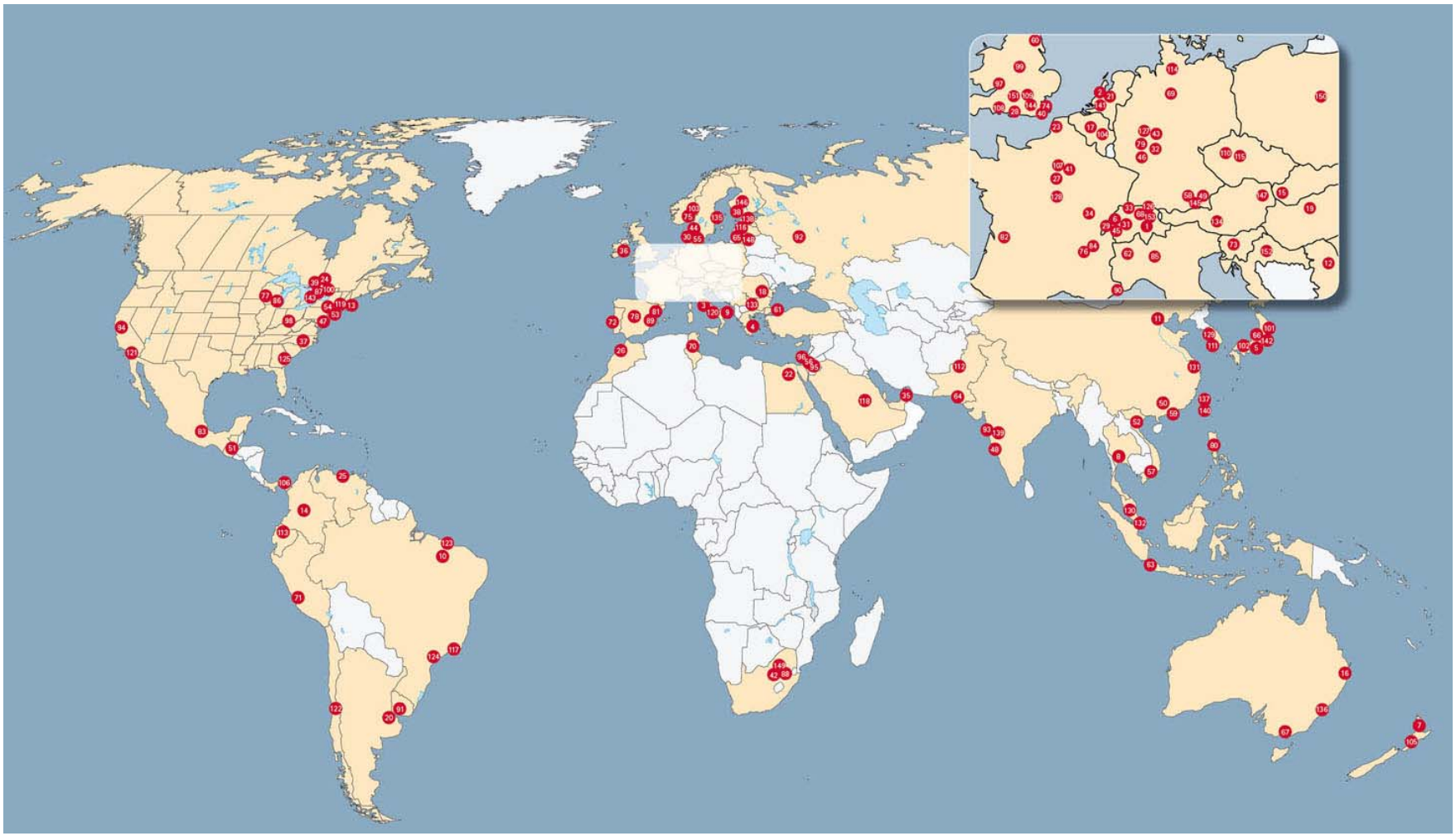
*„Merck Serono“ = former Merck Ethicals division with Serono S.A.
**The Generics division is currently being divested

Merck Group

- Sales Jan. – June 2007 € 3.5 billion
- Operating result Jan. – June 2007 € 0.5 billion
- Employees worldwide around 30,000
- 242 companies
  in 63 countries
- 61 production sites
  in 26 countries

Locations of the Merck Group

Update June, 30 2007



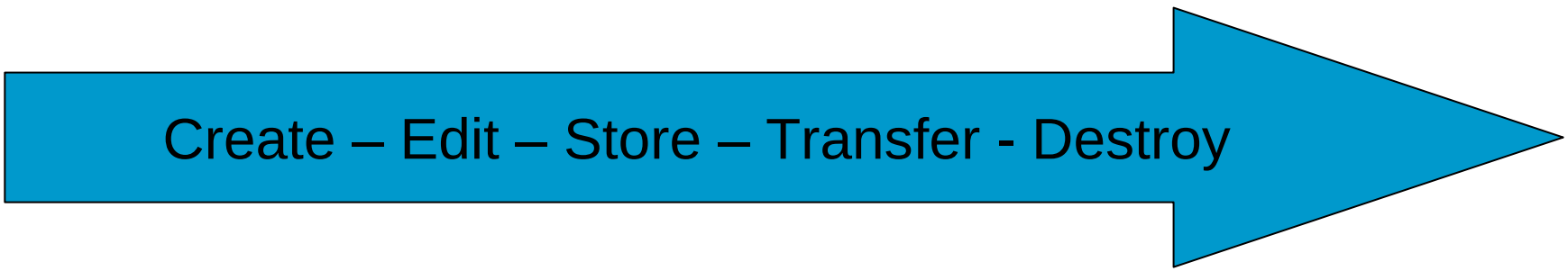
Importance of Information Security

- Information is an asset which, like other important business assets, has value to companies and consequently needs to be suitably protected.
- Information can exist in many forms: paper, electronically, films, spoken words, etc.
- Whatever form it takes and throughout the whole lifecycle of the information, it must always be appropriately protected.

Information Lifecycle

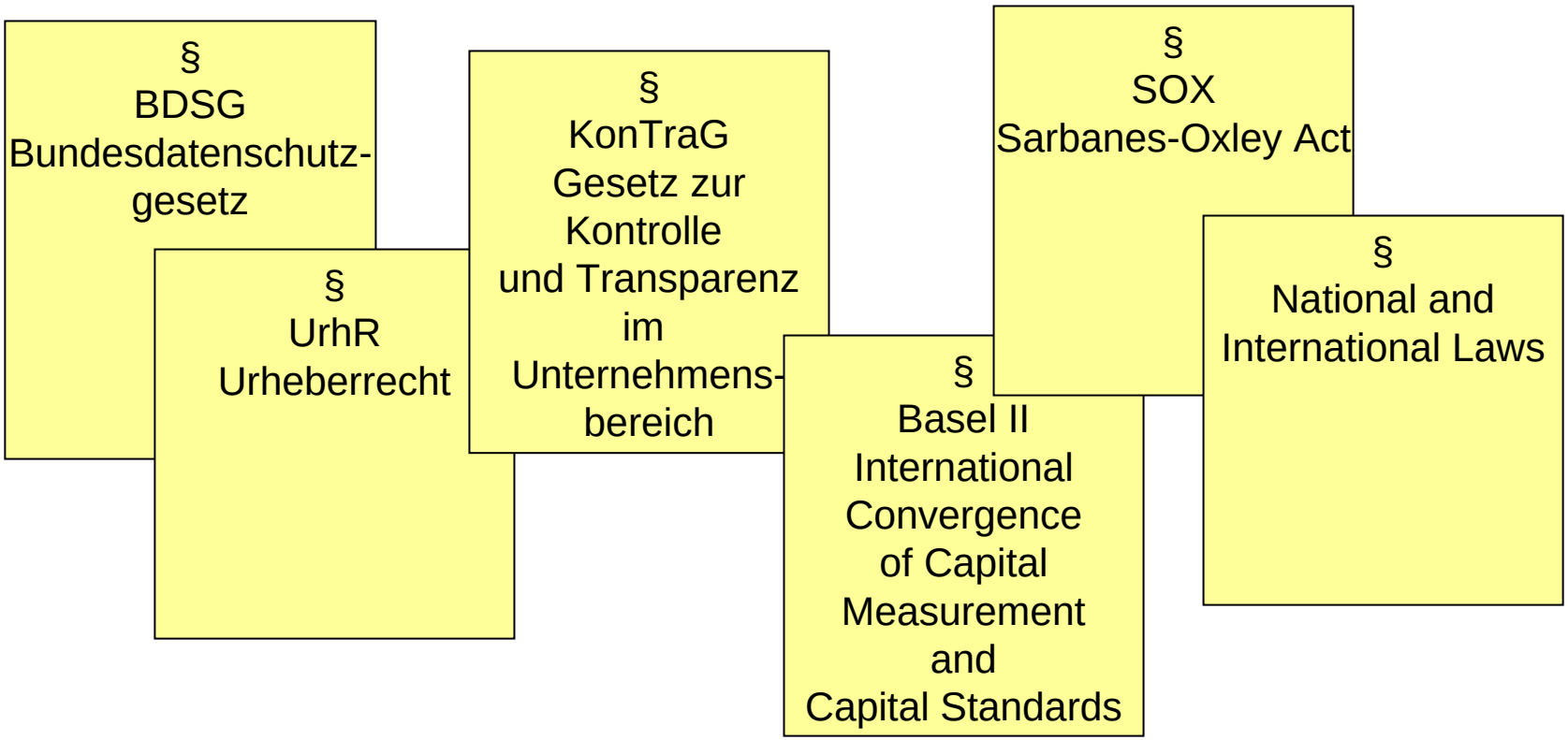
Meeting Minutes Network Plans Formulas Applications
Conferences Presentations Strategic Plans …

E-Mail Paper Notebook Fax Phone PC Server
Video CD Mobile Phone Whiteboard Waste Basket …



More Requirements for Information Security

But there is not only the company's own requirement for Information Security. There are several other requestors.



Scope of Information Security

Information Security

- ensures that information is accessible only to those authorized to have access (confidentiality)
- safeguards the accuracy and completeness of information and processing methods (integrity)
- ensures that authorized users have access to information and associated assets when required (availability)

Threats

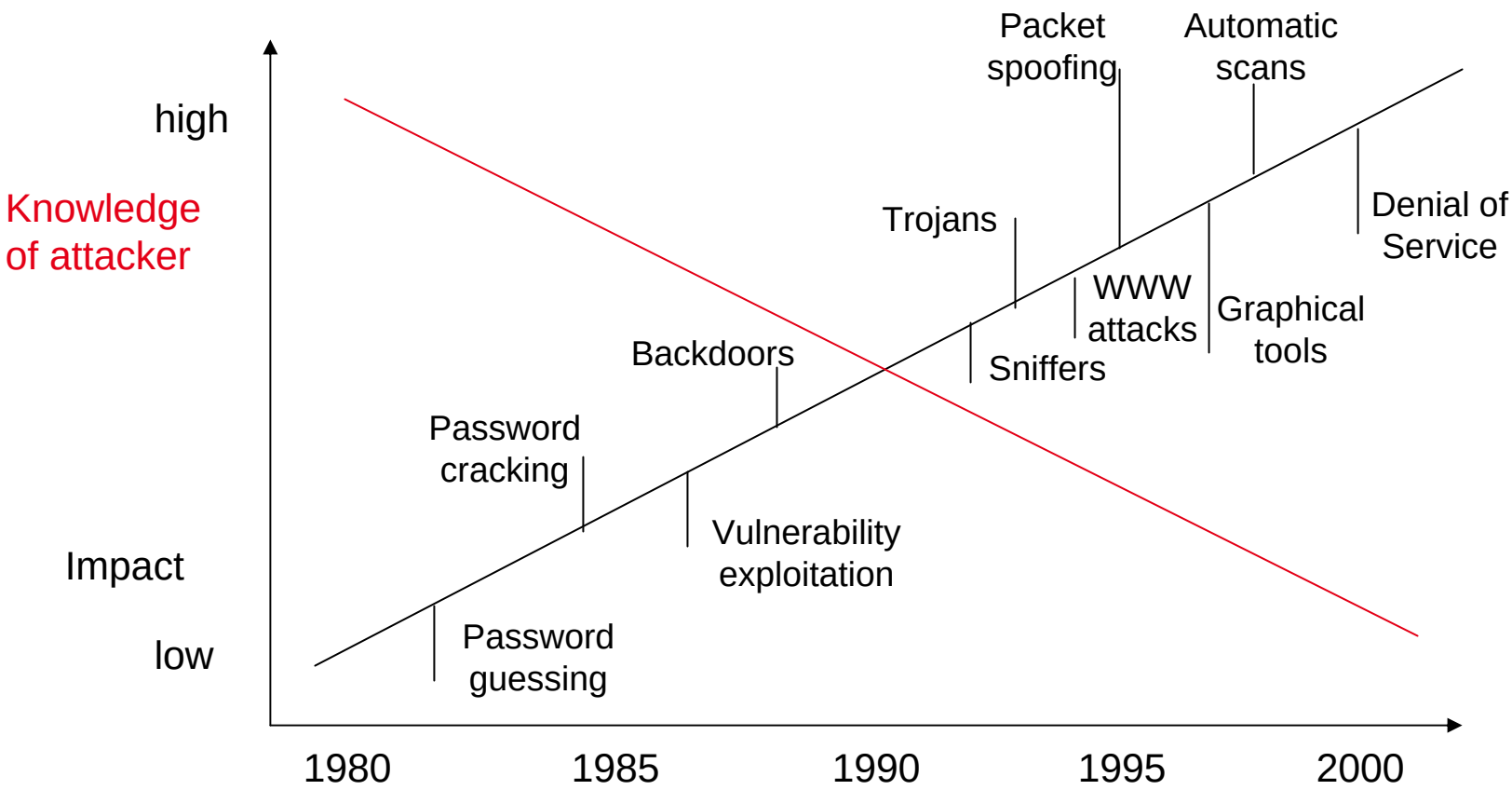
Information Security protects information from a wide range of threats in order to ensure business continuity, minimize damage and maximize return on investment.

Keep in mind:
Threats can be caused by external and by internal attackers.

Example for Threats

- Attacker copies Notes ID file from XCHANGE directory on server, uses a password cracking tool and gains full access to the Notes mailfile of an employee.
- Notebook with unencrypted confidential information is stolen from a hotel room.
- Password for a database is gathered by attacker by social engineering.
- Unencrypted e-mails with confidential information are intercepted by attacker.

Evolution of Threats



Information Security Policy

- The obligatory framework for the implementation of a common level of information security within a company
- Should be based on ISO standards (e.g. ISO 27001)
- Should be approved by management board (not only IT management)
- All employees and business partners must be obliged that their activities comply with this policy
- The policy compliance audit should be part of internal audits

Information Security Policy

Management Policies	Part 1	IT Security Management and Organization Security Policy
	Part 2	Data Privacy, Data Classification and Information Handling Policy
Technical Policies	Part 3	Infrastructure and Facility Security Policy
	Part 4	Software Security Policy
	Part 5	Network Security Policy
	Part 6	IT System Management and Server Security Policy
	Part 7	Personal Computer Security Policy
	Part 8	Telecommuting and Mobile Computer Security Policy
	Part 9	E-Mail Security Policy
	Part 10	Internet-/Intranet Security Policy
	Part 11	Telecommunication Security Policy

Information Security Policy

- There should be a nominated team to review and update the Information Security Policy regularly.
- For unclear situations the team could make appropriate notifications until the next review.
- Most important:
  The Information Security Policy must be documented and accessible for all employees.

Information Security Organization

Corporate Information Security Officers
Corporate Information Security Team (CIST)

Regional Information Security Coordinators
Europe, Latin America, North America, Asia

Local Information Security Officers
Each company of the group nominated a
Local Information Security Officer

Information Security Organization

Local Management is appointed to take overall responsibility for:

- development and implementation of information security
- supporting the identification of controls

The operational tasks could be delegated to the Local Information Security Officer.

All employees are obliged that their activities comply with the policy.

Information Security Organization

- It is a good idea to separate the strategic and the operational Information Security Organizations

Information Security Awareness

Corporate Merck Information Security Policy
Part 1: IT Security Management and Organization Policy

I-§48 All employees of the organization and, where relevant, third-party users, shall receive appropriate training and regular updates in organizational policies and procedures. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities, e.g. log-on procedures, use of software packages, before access to information or services is granted.

ISO 17799 Compliance: Chapter 6.2.1

Information Security Awareness

Corporate Merck Information Security Policy
Part 1: IT Security Management and Organization Policy

I-§6 The Local Information Security Officer supports the local management in all kind of needs related to information security. Especially, he

[…]

c) agrees and supports organization-wide information security initiatives, e.g. security awareness program;

ISO 17799 Compliance: Chapter 4.1.2

Information Security Awareness

To fulfill the requirements of the Corporate Information Security Policy two major elements are employed:

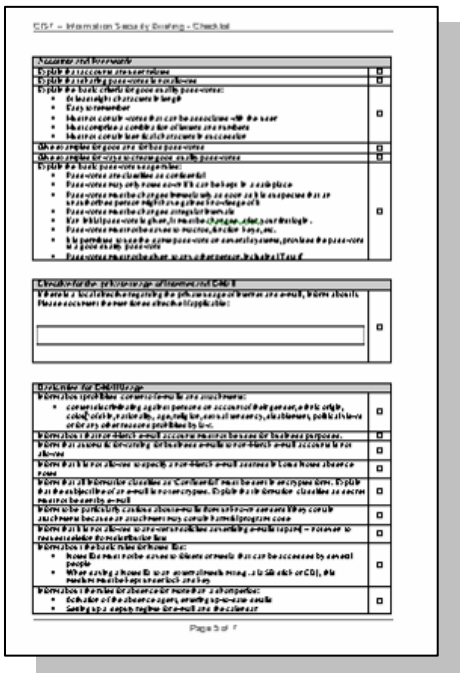
Information Security Briefing	InfoSec Basic Training
Short information about most important topics. Duration: ~30 min.	Detailled information about topics contained in InfoSec Briefing and additional topics. Duration: ~120 min.
- Why Information Security? - Classification of Information - Basic Rules for Information Security - Accounts and Passwords - Private Use of Merck Systems - Basic Rules for E-Mail Usage - HW/SW Installation - Mobile Systems - Copyright / Intellectual Property	- Why Information Security? - Corporate Information Security Policy - Information Security Roles&Responsibilities - Data Protection - Information Handling Procedures - Password Usage - E-Mail Usage - Mobile Devices - Information Security Incidents

Information Security Awareness

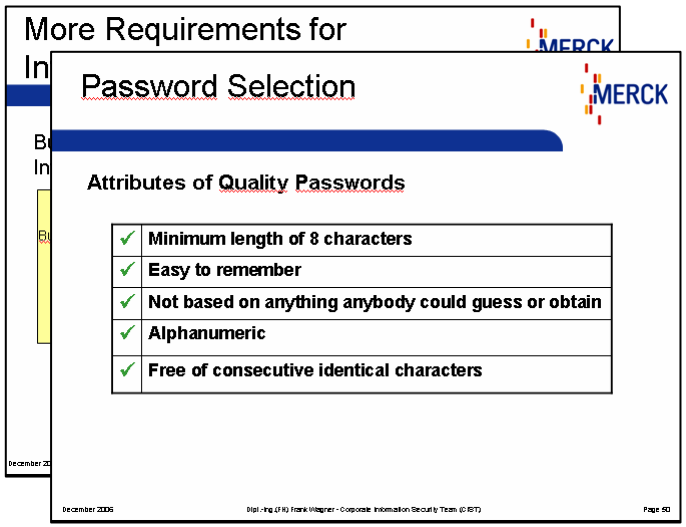
- All employees joining a company of the group must go through an Information Security Briefing.
- The Information Security Training is obligatory for members of Corporate Information Services.
- After the Briefing and the Training the participants must pass an exam.
- The participation must be documented.

Information Security Awareness

Material provided by Corporate Information Security Team:



Information Security
Briefing Document
(incl. Signature Sheet)



Slides

Questionnaire

Certificate

Report Template

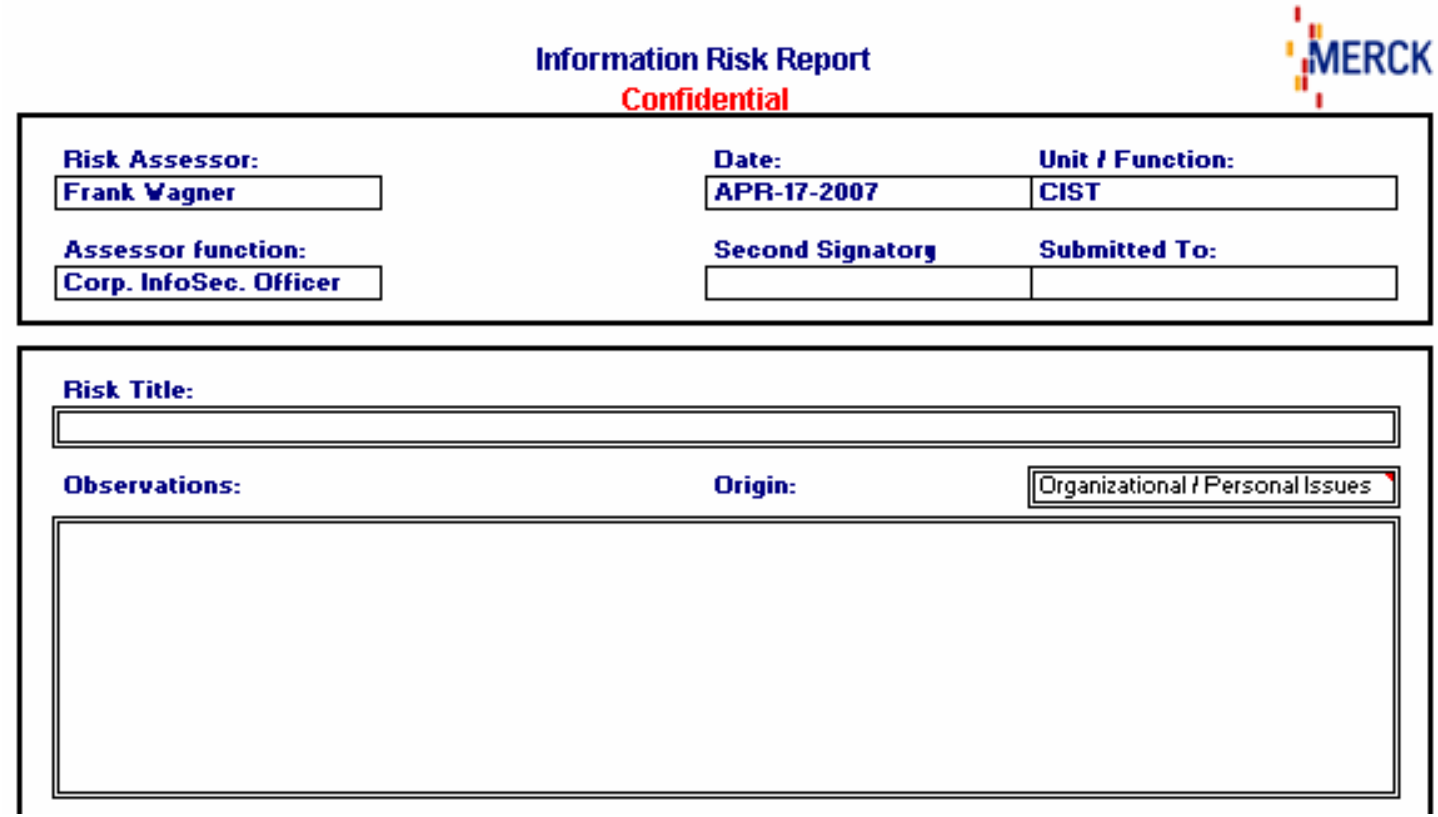
Information Security Audits

- Based on Information Security Audits
- Performed by Corporate Auditing Department and Information Security Department
- Yearly Audit Plan
- Internal and external audits (supplier audits)
- Document audits, on-site audits, pre-audits
- Two auditors
- Audit Report → Corrective Action/Planned Activies Plan
- Review
- Reporting to the management board

Information Security Risk Management

- For every risk a risk assessment is done and documented in an Information Risk Report which is reported to Corporate IS management

Information Security Risk Management



Information Risk Report

Confidential

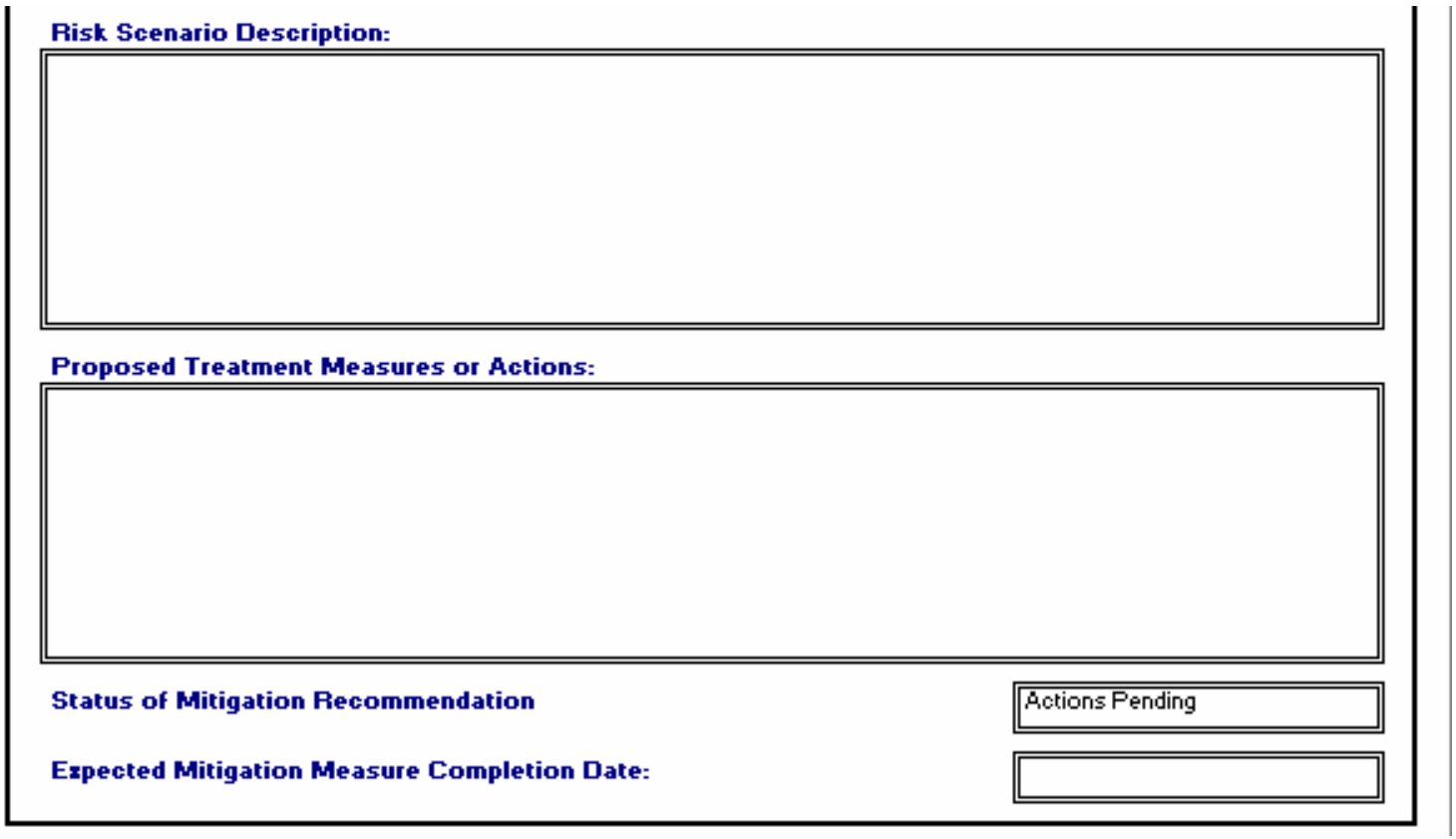
MERCK

Risk Assessor:	Date:	Unit / Function:
Frank Wagner	APR-17-2007	CIST
Assessor function:	**Second Signatory**	**Submitted To:**
Corp. InfoSec. Officer		

Risk Title:

Observations: **Origin:** Organizational / Personal Issues

Information Security Risk Management



Information Security Risk Management

Threat Likelihood	
People - non intentional	0
People - intentional	2
Technical failure	1
Environment related	0
Neighborhood	0
Organization	2

Impact	
Strategy	0
Financial	2
Customer	1
Legal / Compliance	3
Image / Reputation	3
Security (CIA)	2

Risk Evaluation:

Current Risk Impact:	3	(0-4 as per risk matrix)
Current Risk Likelihood:	4	(0-4 as per risk matrix)
Mitigated Risk Impact:	2	(0-4 as per risk matrix)
Mitigated Risk Likelihood:	1	(0-4 as per risk matrix)