# IT Incident Management and Structured Documentation
# - Company specific adoption

**Dipl.-Inf. Sandra Frings**
Fraunhofer IAO
Competence Center Software-Management
Sandra.Frings@iao.fhg.de
www.sw-management.iao.fhg.de

IMF 2007





Fraunhofer Institut Arbeitswirtschaft und Organisation

# Definition of Terms
## Documentation - Reporting - Recording

- Writing down content for preserving / presentation / information - e.g.
  - news, letters
  - marekting information

- Writing down on how to do a task - looking into the future - e.g.
  - standard operating procedures
  - guidelines
  - process descriptions
  - handbooks, user manuals
  - lists of requirements

on paper or digital

manually or automatically generated

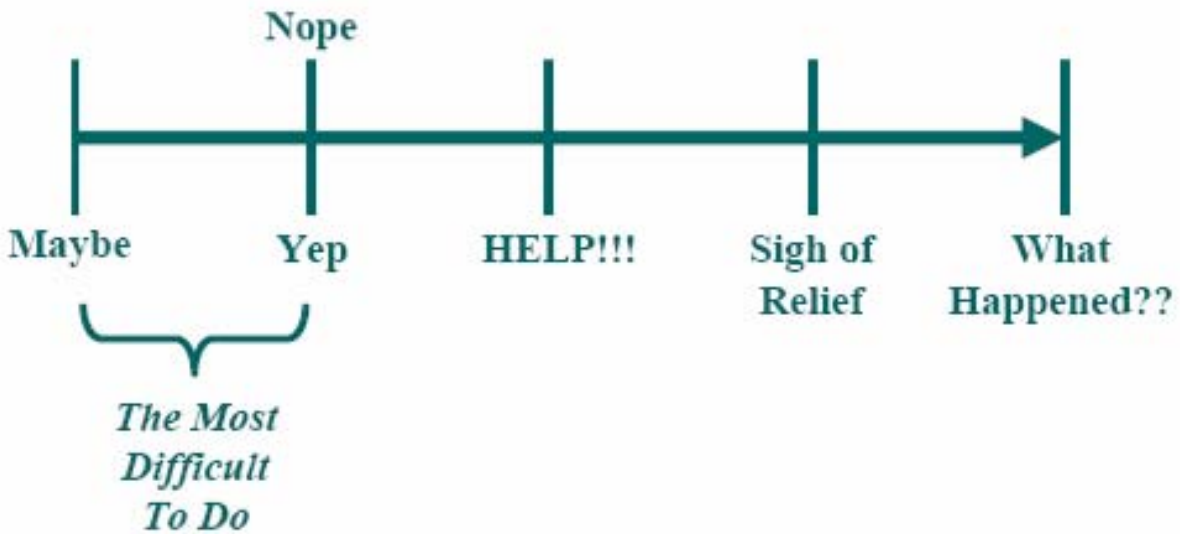
- Writing down what has happened - looking into the past - e.g.
  - log file, log book
  - news, history
  - evidenciary data




Fraunhofer Institut Arbeitswirtschaft und Organisation

# The Situation

## The Continuum of an Incident




Peter R. Stephenson, PhD
CISSP, CISM, FICAF
Norwich University
pstephen@norwich.edu



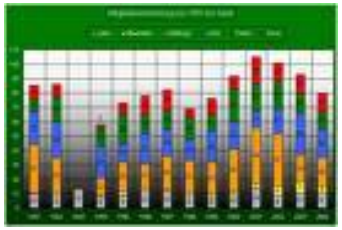


Fraunhofer Institut Arbeitswirtschaft und Organisation

# Why this „Problem“ with IT Related Incidents?

- Computers / electronic devices
  - help commit crimes
  - are (easy) targets of crimes
- Preparedness and „readiness“ mostly not sufficient / appropriate
- What is „appropriate“?
  - no general solution
  - analysis / audits help as a starting point
- Always the „budget problem“ – IT security management is currently still **not** seen as a vital business process.

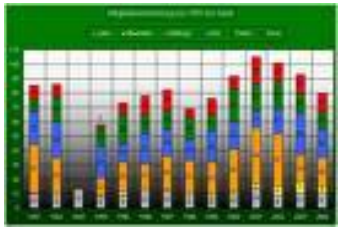
# Statistical Data



- German Federal Criminal Police Office BKA 2006: Overall decline of reported computer related incidents in Germany in 2006 by 4,9%
  - illegally acquired PIN for credit cards -15%
  - software piracy - 28%
  - Counterfeiting and forgery of probative data +143%
  - spy out data +26%
- CSI/FBI Report 2006 -> large organisations
  - virus attacks are unauthorised access - largest source for financial losses
  - increase in reporting computer intrusions - neg. publicity being a problem
  - 80% do security audits
- IDC Survey 2006 -> SME
  - most enterprises neglect the security of computer systems
  - but only 18% had computer related incidents

source: www.bka.de

# Problems with Statistical Data

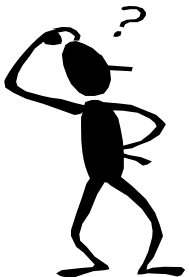


- Question
  - Less incidents OCCURED

  or
  - Less incidents were REPORTED

  or
  - Less incidents were DETECTED?

source: www.bka.de







Fraunhofer Institut Arbeitswirtschaft und Organisation

# Requirements Resulting from Identified Problems

- awareness
- IT-security management (incl. emergency plan / contingency plan)
- training in the area of IT-security
- documented procedures and guidelines for incident management / response in organisations
- collection of electronic evidence
- analysis of data
- cooperation and communication (national and international)
- diversity of laws
- presentation of electronic evidence to court
- standardised reporting of incidents
- lack of documentation which is complete
- lack of “organised” documentation and reporting

# Presentation Objectives

**Making *organisations* understand that ...**

- ... selective problem solving ...
- ... spontaneous problem solving ...
- ... unqualified problem solving ...
- ... purely technological solutions to solve a problem ...
- ... undocumented problem solving ...

**... will not suffice!**

IMF 2007





Fraunhofer Institut Arbeitswirtschaft und Organisation

# Presentation Objectives

**Making *organisations* understand that ...**

- ... selective problem solving ...
  -> holistical approach
- ... spontaneous problem solving ...
  -> preparation
- ... unqualified problem solving ...
  -> qualification
- ... purely technological solutions to solve a problem ...
  -> organisation
- ... undocumented problem solving ...
  -> documentation and reporting

**instead we need...**

IMF 2007





Fraunhofer Institut Arbeitswirtschaft und Organisation

# General Advantages of Documentation

- Supports searching and finding information
- Supports tracing who did what when how and why (especially if the time between incident and investigation is rather large)
- Base for quality management - required by ISO 9000 anyway
- Process improvement: e.g. safe time and money searching for information
- Supports know-how transfer (planned for new employees and e.g. third party people especially if no separate company investigation experts/unit exist, spontaneous in case of e.g. illness)
- Integration into work flow: prompt provision with appropriate documents
- Common and documented terminology

# My Work

**Introducing an approach for ...**

- ... creation of a concept
  ... adoption of a concept to organisation‘s requirements and needs
  -> WHAT
- ... improvement of processes quality and
  ... support of business continuity
  -> WHY
- ... integration of adequate roles having sound / required qualification
  -> WHO
- ... stepwise approach
  -> HOW
- ... being ready
  -> WHEN

# State of the Art – IT Security Management

- security safeguards and implementation advice within the German BSI Baseline Protection Manual,
- standards like the ISO 17799:2005 - Code of practice for information security management,
- or the ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems – Requirements,
- technical reports like the ISO/IEC TR 18044:2004 - Information Technology - Security Techniques - Information Security Incident Management,
- procedures like the ACPO Good Practice Guide for Computer Based Electronic Evidence,
- best practices like IT Infrastructure Library Security Management,
- judicial guidelines like the Convention on Cyber Crime,
- guideline like the NIST Incident Handling Guide,
  - Microsoft's incident response process
  - and many more ...

# State of the Art – IT Security Management

- security safeguards and implementation advice within the German BSI Baseline Protection Manual,
- standards like the ISO 17799:2005 - Code of practice for information security management,
- or the ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems – Requirements,
- technical reports like the ISO/IEC TR 18044:2004 - Information Technology - Security Techniques - Information Security Incident Management,
- procedures like the ACPO Good Practice Guide for Computer Based Electronic Evidence,
- best practices like IT Infrastructure Library Security Management,
- judicial guidelines like the Convention on Cyber Crime,
- guideline like the NIST Incident Handling Guide,
  - Microsoft's incident response process
  - and many more ...

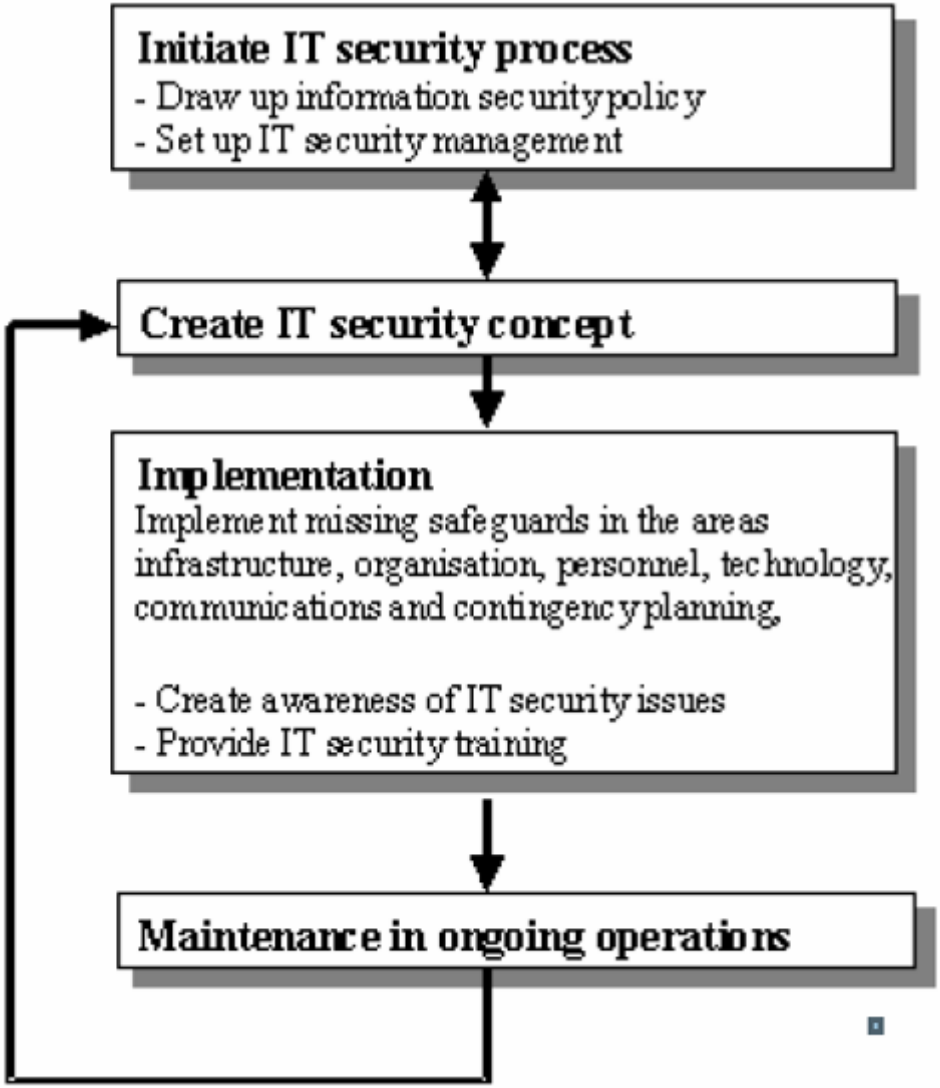
Adopting new processes means need in available

- budget
- people
- organisation
- technology




Fraunhofer Institut Arbeitswirtschaft und Organisation

# BSI Baseline Protection Manual (2004) - as Example



# Taking a detailed look at the State of the Art
## Focussing on documentation

– Looking at „available help“ there is a **demand** for documentation EVERYWHERE!

Why? „There must be some kind of benefit...“

Why **not**?

– “Documentation is a hassle”
– “Documentation does not make money
– “Documentation is useless and a waste of paper”

What are documentations requirements?

# Documentation Requirements

Source: Functional Requirements for Evidence in Recordkeeping: The Pittsburgh Project

- Digital information has to satisfy the requirements "integrity", "authenticity", "reliability" and "archiving"

- Comprehensive (suited for the target reader)
- Identifiable
- Complete
  - Accurate
  - Understandable
  - Meaningful and reasonable
- Authorized
- Preserved
  - Inviolate
  - Coherent
  - Auditable

- Removable
- Exportable
- Accessible
  - Available
  - Renderable
  - Evidential

→ **Structured**




Fraunhofer Institut Arbeitswirtschaft und Organisation

# Example of Expected Reports

Safeguard S2.201 (of German Baseline Protection Manual) states that the documentation should as a minimum extend to the following:

- Information security policy,
- Schedules of IT assets (including connectivity plans etc.),
- IT security concept(s),
- Plans for implementation of IT security measures,
- Procedures for the proper and secure use of IT facilities,
- Documentation of reviews (checklists, interview notes etc.),
- Minutes of meetings and decisions made by the IT security management team,
- Management reports on IT security,
- IT security training plans, and
- Reports on security-relevant incidents.

# Example of Documentation Guideline

In Safeguard 6.64, the documentation guideline for an incident goes as far as:

"All actions performed while dealing with a security problem should be documented in as much detail as possible so as to

- retain the details of what happened,
- make it possible to retrace the problems which occurred,
- be able to rectify any problems/faults which could result from hasty implementation of countermeasures,
- be able to resolve problems already known more quickly should they occur again,
- be able to eliminate the security weaknesses and draw up preventive measures,
- collect evidence if a prosecution is to be brought.
  Such documentation includes not only a description of the actions carried out including the times at which they were taken, but also the log files of the affected IT systems."

# Example of Documentation Guideline

In Safeguard 6.64, the documentation guideline for an incident goes as far as:
"All actions performed while dealing with a security problem should be documented in as much detail as possible so as to

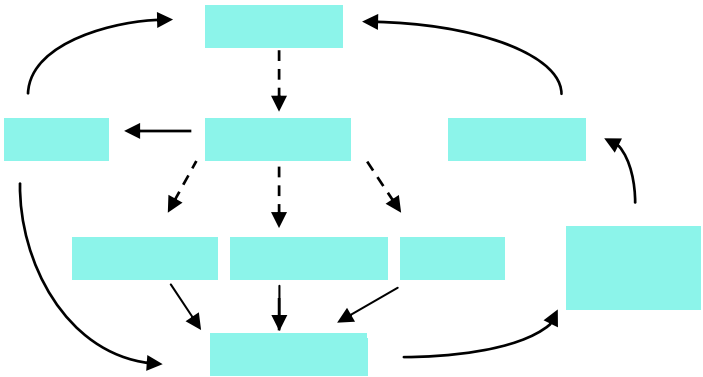
- retain the details of what happened,
- make it possible to retrace the problems which occurred,
- be able to rectify any problems/faults which could result from hasty implementation of countermeasures,
- be able to resolve problems already known more quickly should they occur again,
- be able to eliminate the security weaknesses and draw up preventive measures,
- collect evidence if a prosecution is to be brought.
  Such documentation includes not only a description of the actions carried out including the times at which they were taken, but also the log files of the affected IT systems."

BUT

- How can the requirements be met?
- What is the target group?
- What is the structure?

# Demand for a holistic Method

- Holistic and process oriented approach
- Structured according to IT security management and IT incident management processes defined within the organisation
- Results for different target groups



IMF 2007





Fraunhofer Institut Arbeitswirtschaft und Organisation

# Technical Solution?
## Electronic Records Management Systems

ISO 15489:2001 - Information and documentation -- Records management

- setting policies and standards
- assigning responsibilities and authorities
- establishing, enforcing and publishing procedures and guidelines
- providing a range of services relating to the management and use of records
- designing, implementing and administering specialized systems for managing records, and
- **integrating records management into business systems and processes**

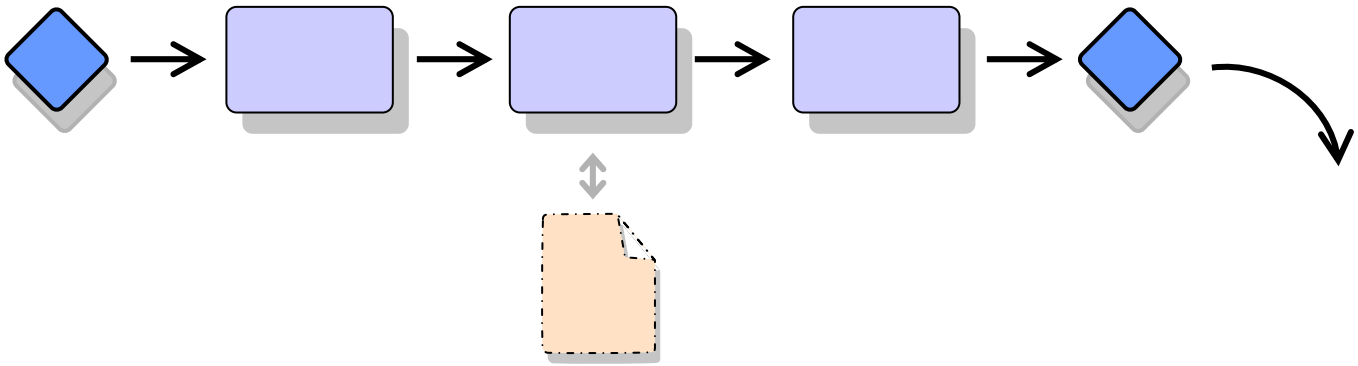
Source: http://en.wikipedia.org/wiki/Records_Management

# Technical Solution?
## Document Management and Work Flow Management Systems

| | |
|---|---|
| **Retrieval** | Typically via a built in search engine. Some also allow documents to be retrieved using metadata (date, time, tags, document type, etc) |
| **Filing** | Organization? Strategy? |
| **Security** | Protection against loss, tampering or destruction of documents? How to deal with sensitive information? |
| **Archival** | Readability? How can we protect our documents against fires, floods or natural disasters? |
| **Retention** | What to retain? Length of retention? Removal? |
| **Distribution** | People? Cost of distribution? |
| **Workflow** | If documents need to pass from one person to another, what are the rules for how their work should flow? |
| **Creation** | Number of people and logistics of collaboration? |
| **Authentication/Approval** | How do we provide needed requirements for legal submission to government and private industry that the documents are original and meet their standards for authentication? |

Source: http://en.wikipedia.org/wiki/Document_management_system

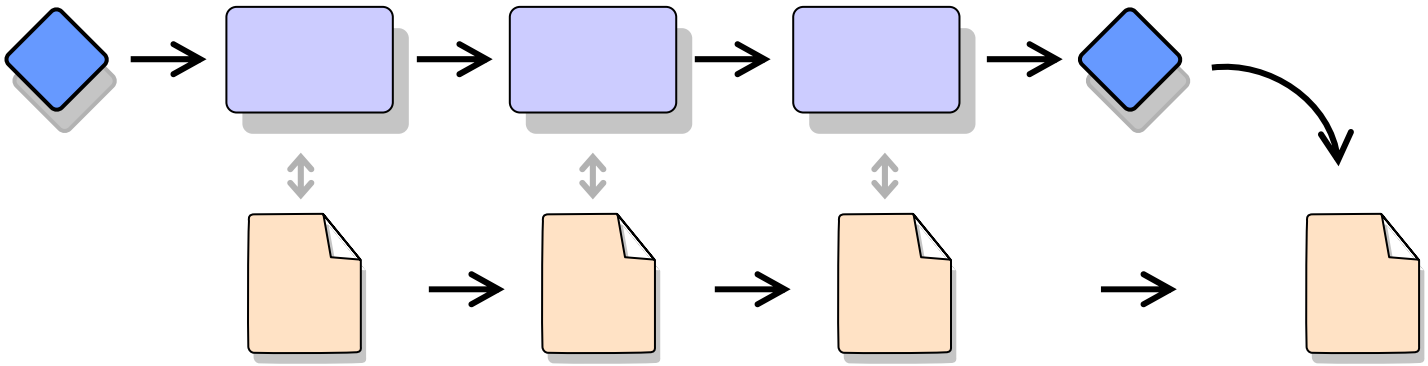
# Document and Records Management
## Current Status






Fraunhofer Institut Arbeitswirtschaft und Organisation

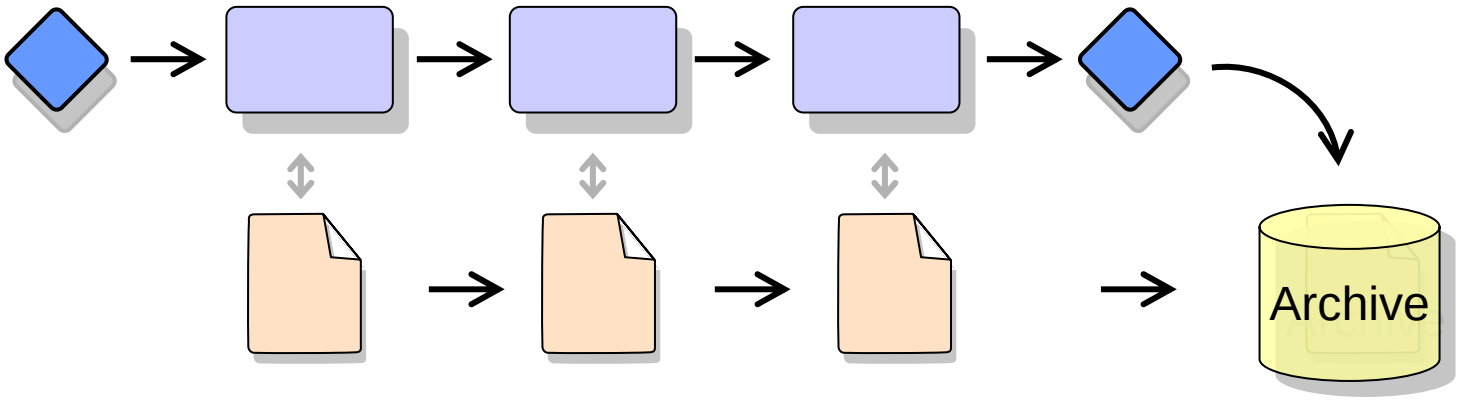
# Document and Records Management
## Current Status



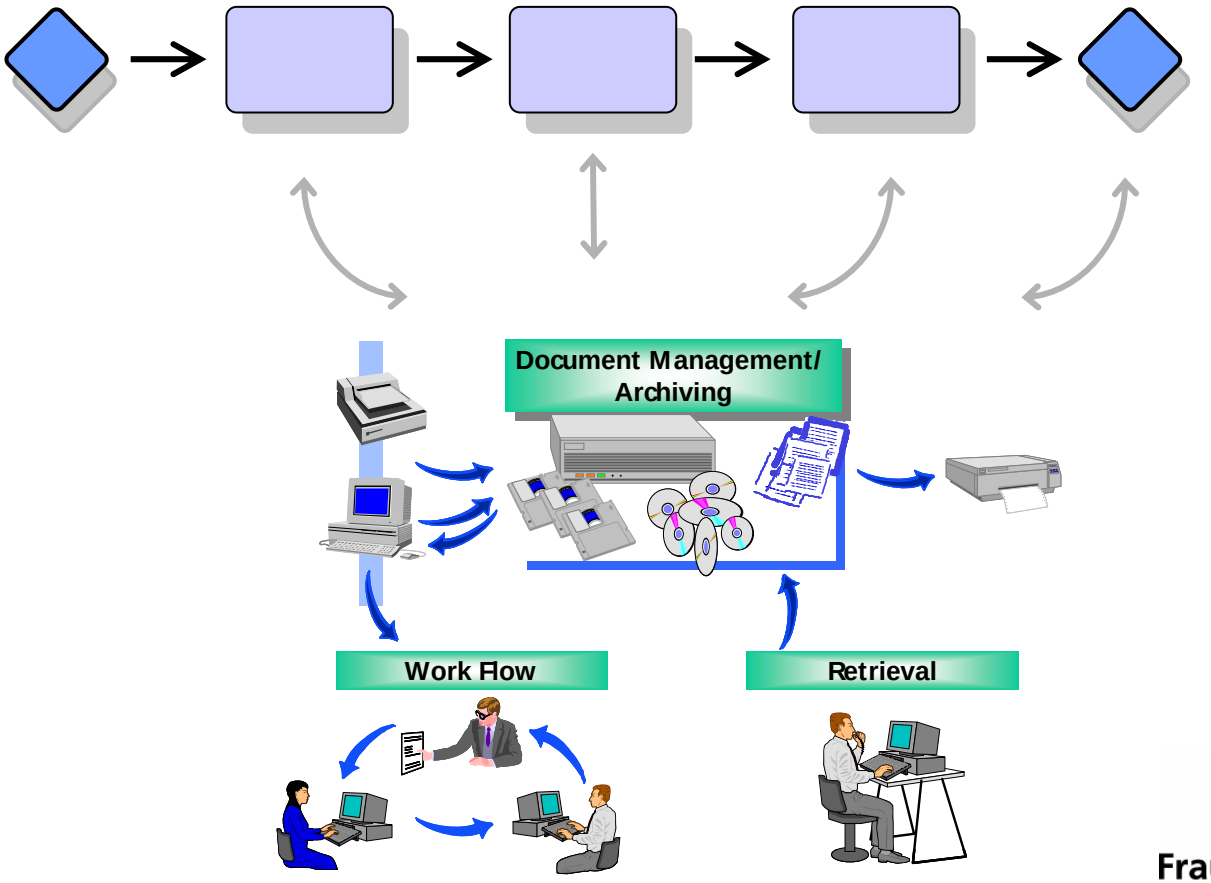



Fraunhofer Institut Arbeitswirtschaft und Organisation

# Document and Records Management
## Current Status



# Document and Records Management
## Planned Situation

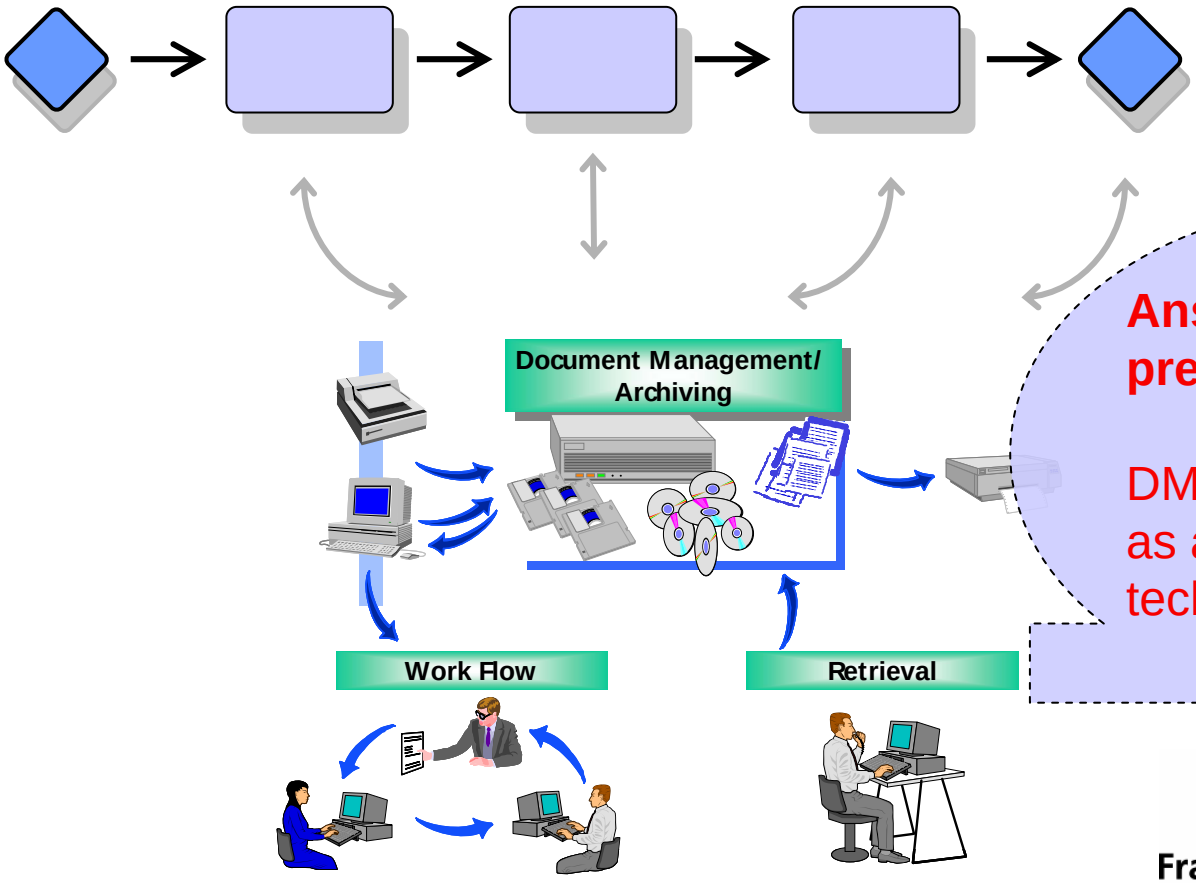






Fraunhofer Institut Arbeitswirtschaft und Organisation

# Document and Records Management
## Planned Situation




**Answer to a previous question:**

DMS / ERMS / WFMS as a component of the technical solution




Fraunhofer Institut Arbeitswirtschaft und Organisation

# Initial Situation in an Organisation (especially SME)

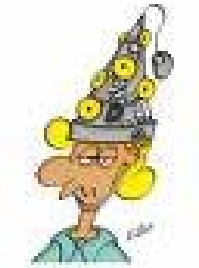
Processes

Require-
ments

Hand-
books

Guide-
lines

Expert



DAU /
Newbie

Policies

Contacts

Responsi-
bilities

Software
Systems

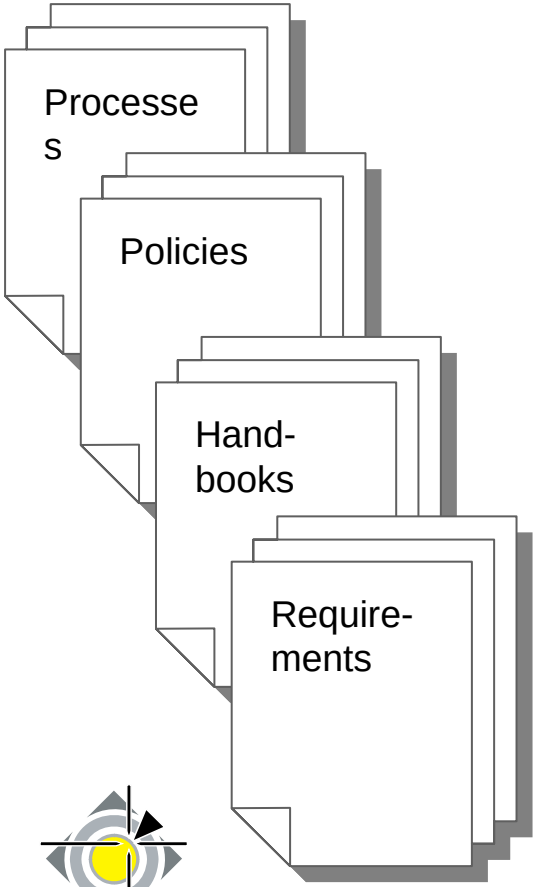
IMF 2007

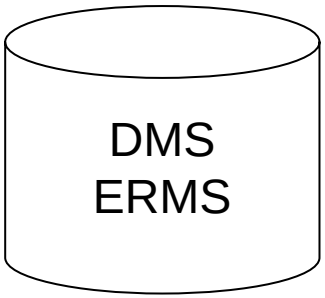




Fraunhofer Institut Arbeitswirtschaft und Organisation

# Method for Structured Documentation



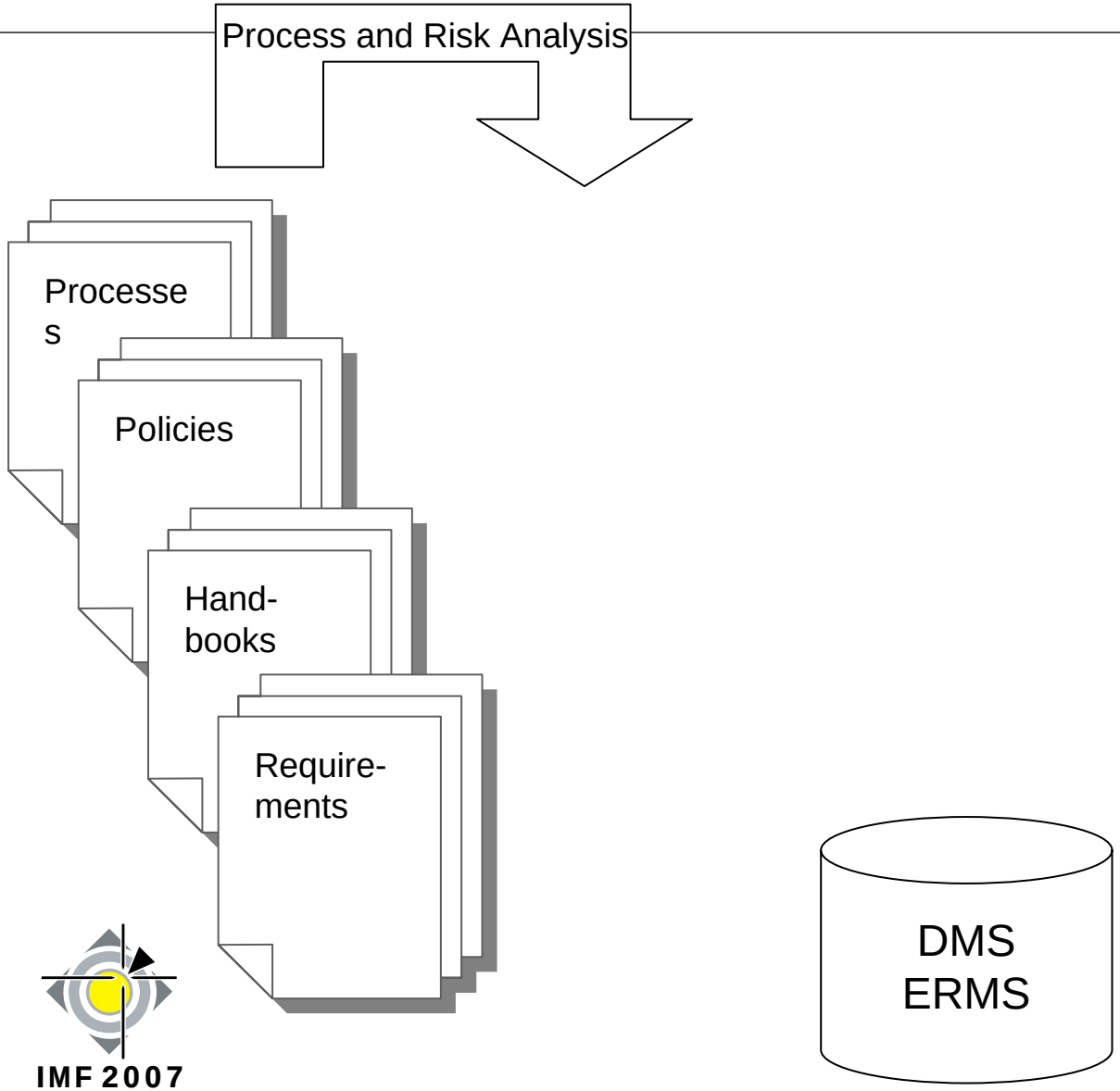

IMF 2007





Fraunhofer Institut Arbeitswirtschaft und Organisation

# Method for Structured Documentation



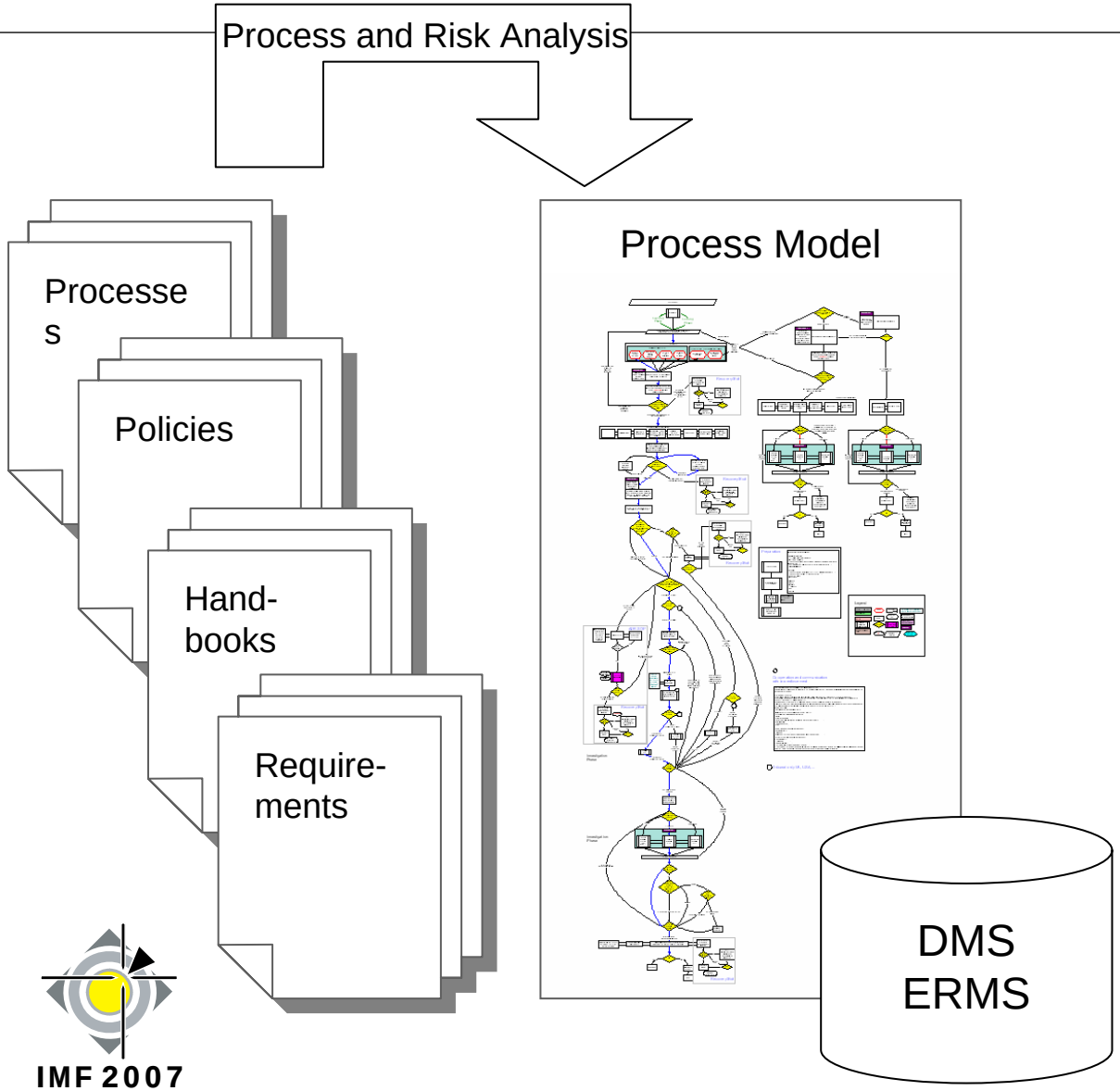

IMF 2007





Fraunhofer Institut Arbeitswirtschaft und Organisation

# Method for Structured Documentation

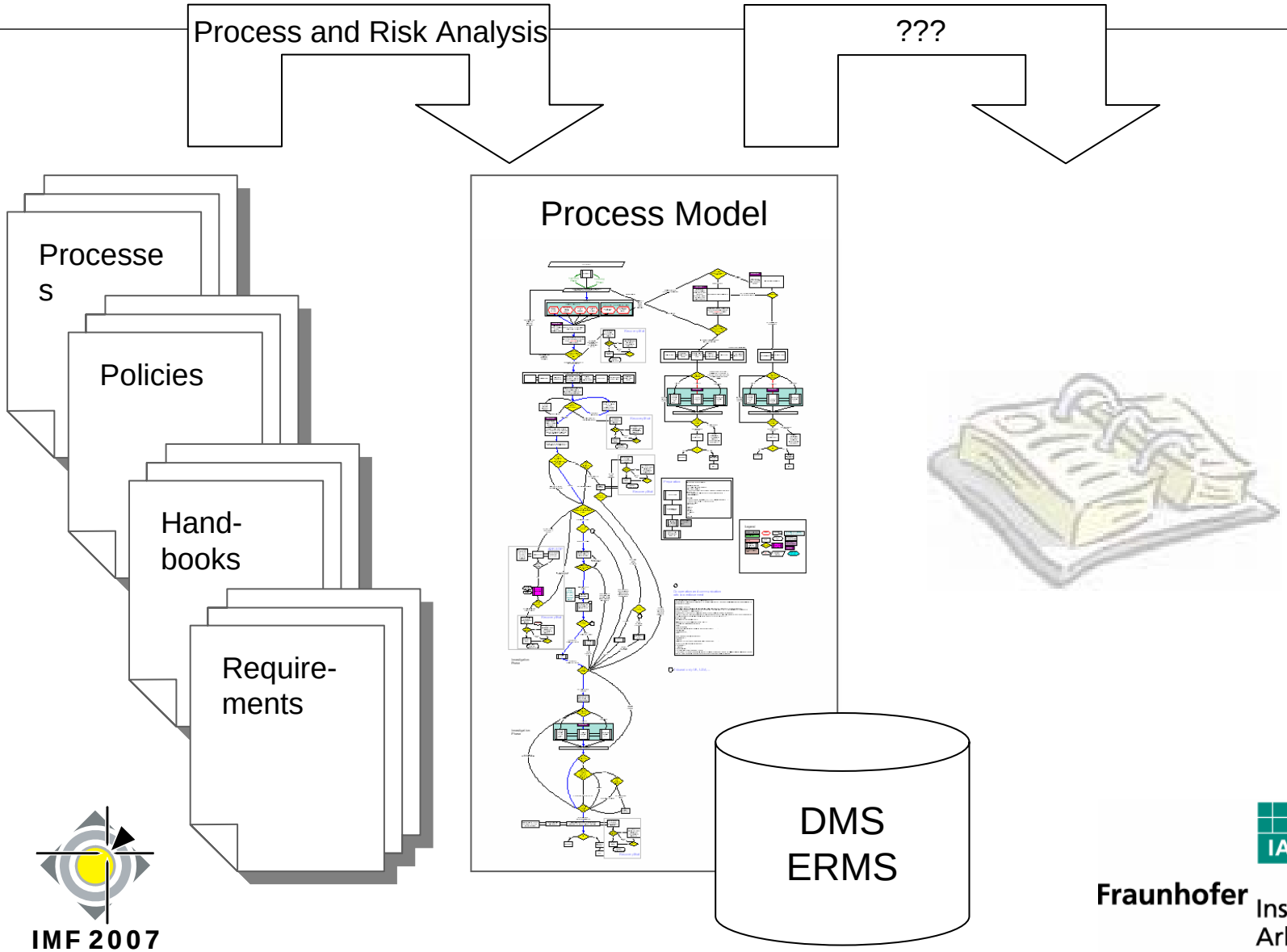






Fraunhofer Institut Arbeitswirtschaft und Organisation

# Method for Structured Documentation







Fraunhofer Institut Arbeitswirtschaft und Organisation

# Method for Structured Documentation

Process and Risk Analysis

„Automated“ Generation

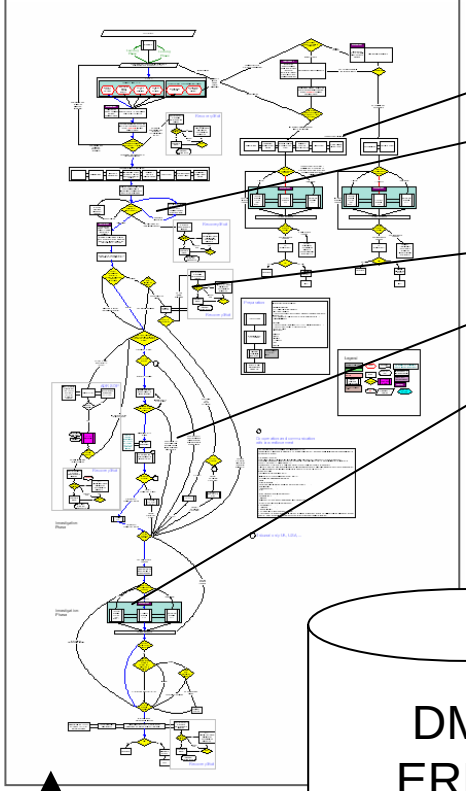
Processes

Policies

Hand-books

Require-ments

WFMS



XML Document

DMS
ERMS





Fraunhofer Institut Arbeitswirtschaft und Organisation

# Method for Structured Documentation

Process and Risk Analysis

„Automated“ Generation

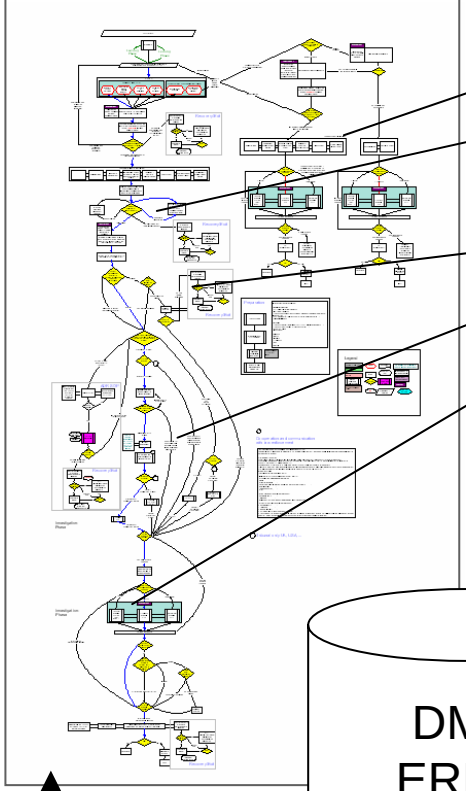
Processes

Policies

Hand-books

Require-ments

WFMS



XML Document

Overall written structured Documentation

- Preparation
- Investigation
- Post Processing

DMS
ERMS

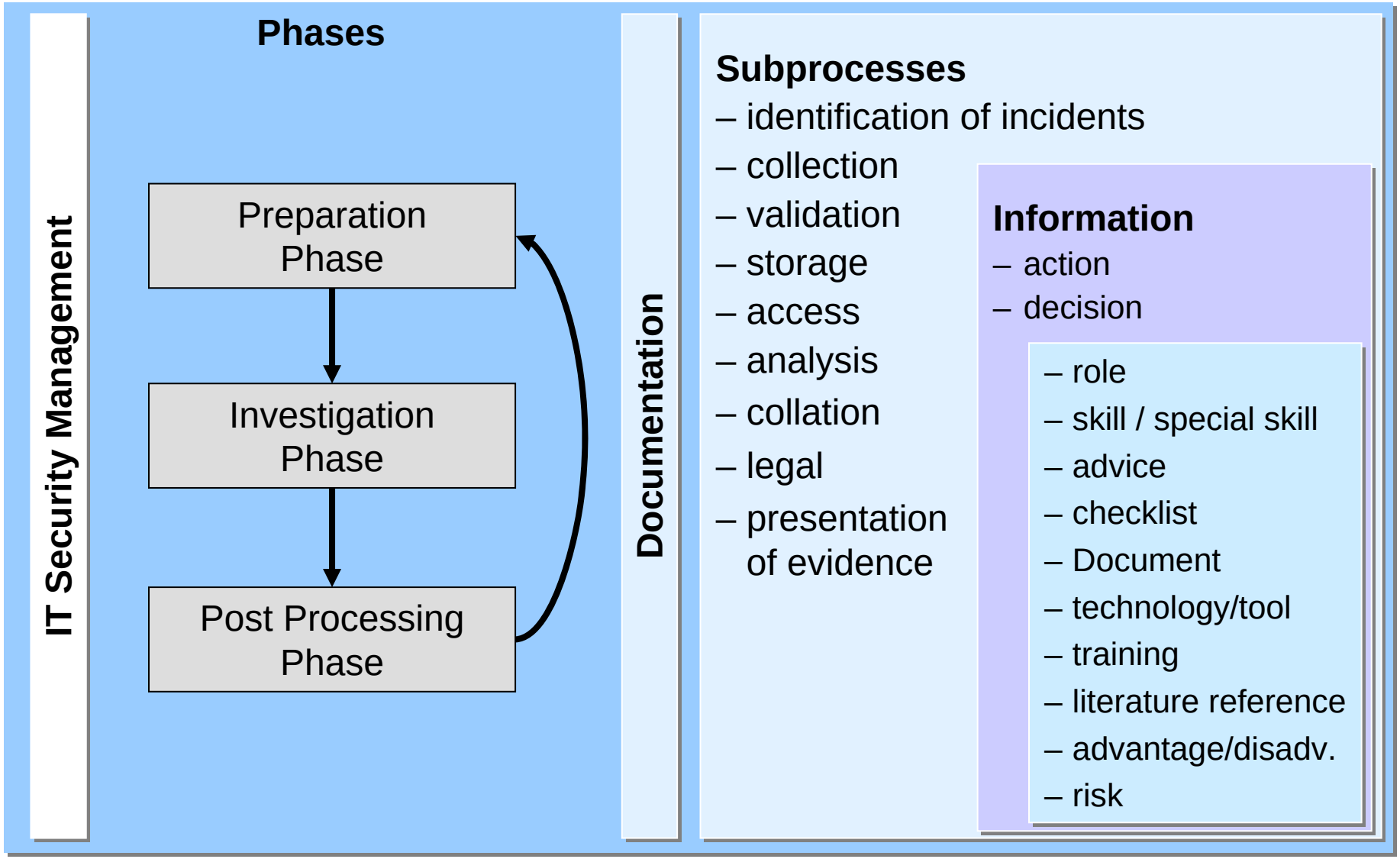
IMF 2007



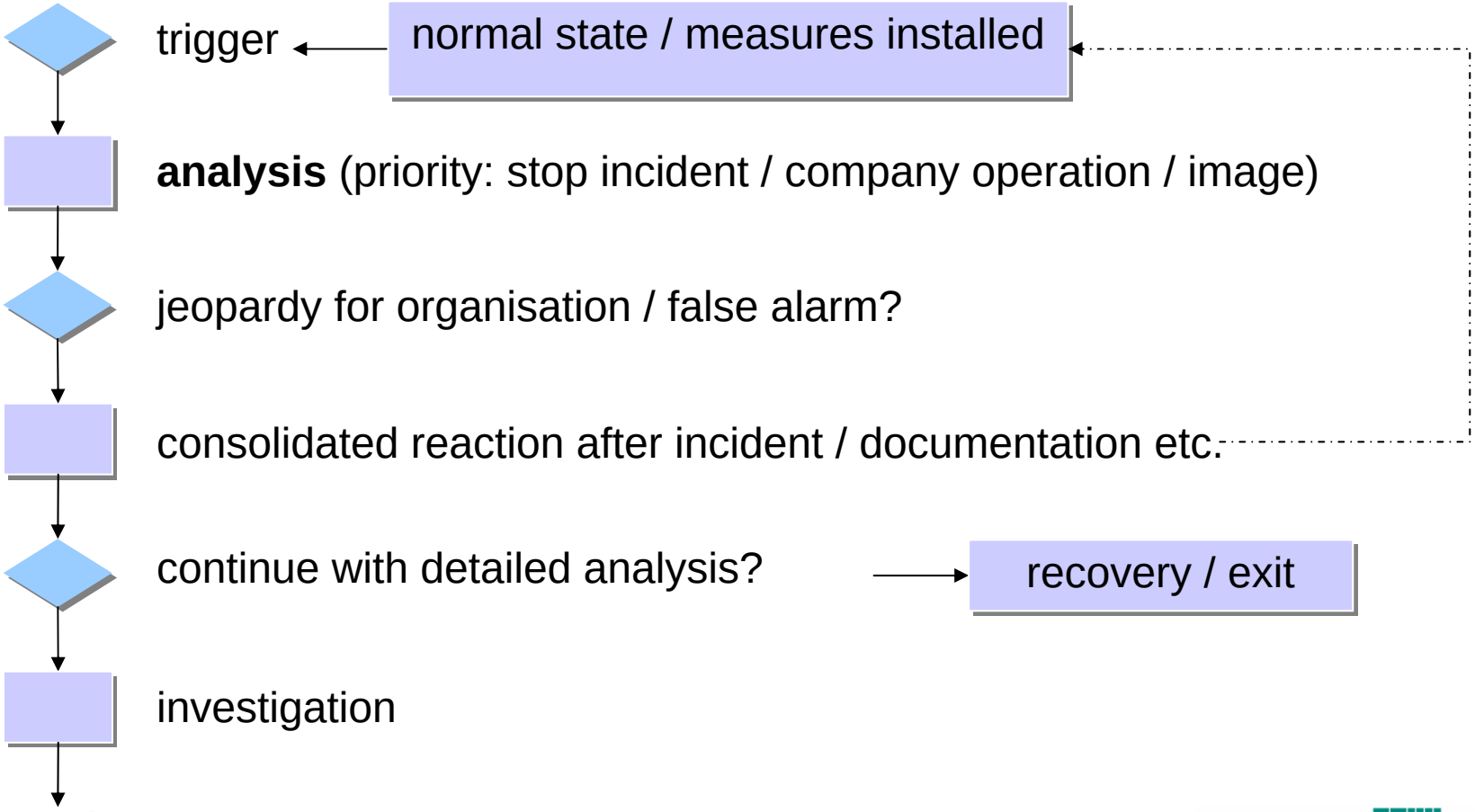


Fraunhofer Institut Arbeitswirtschaft und Organisation

# Components of an IT Incident Management Process Model



# Example

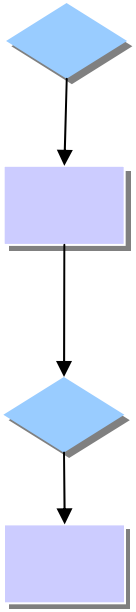






Fraunhofer Institut Arbeitswirtschaft und Organisation

# Example



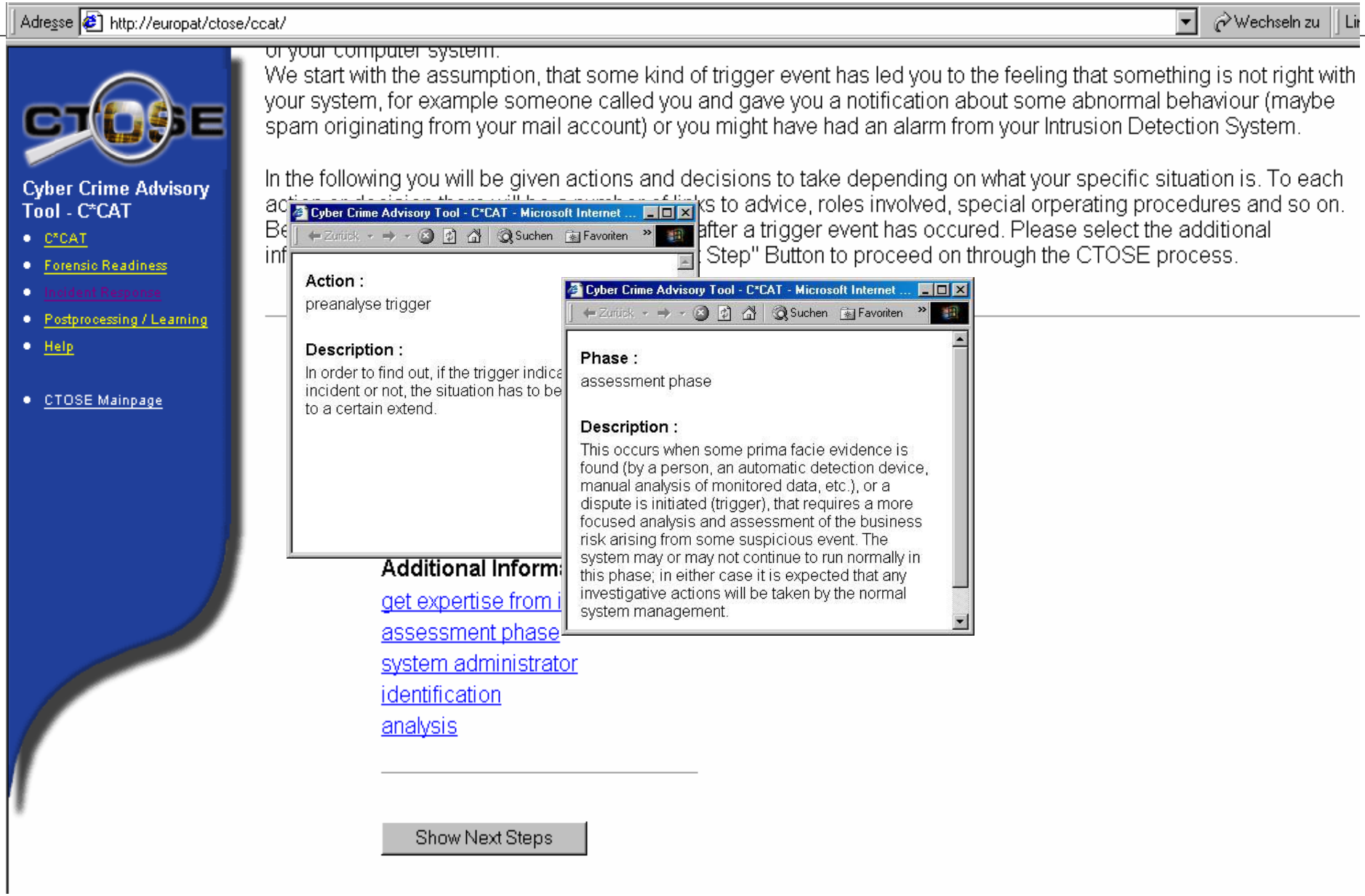
suspect, crime, kind of standards of proof required
for evidence, involve LE?

work together with experts / LE, collect / secure electronic evidence
(SOP of IT-forensic experts / LE)

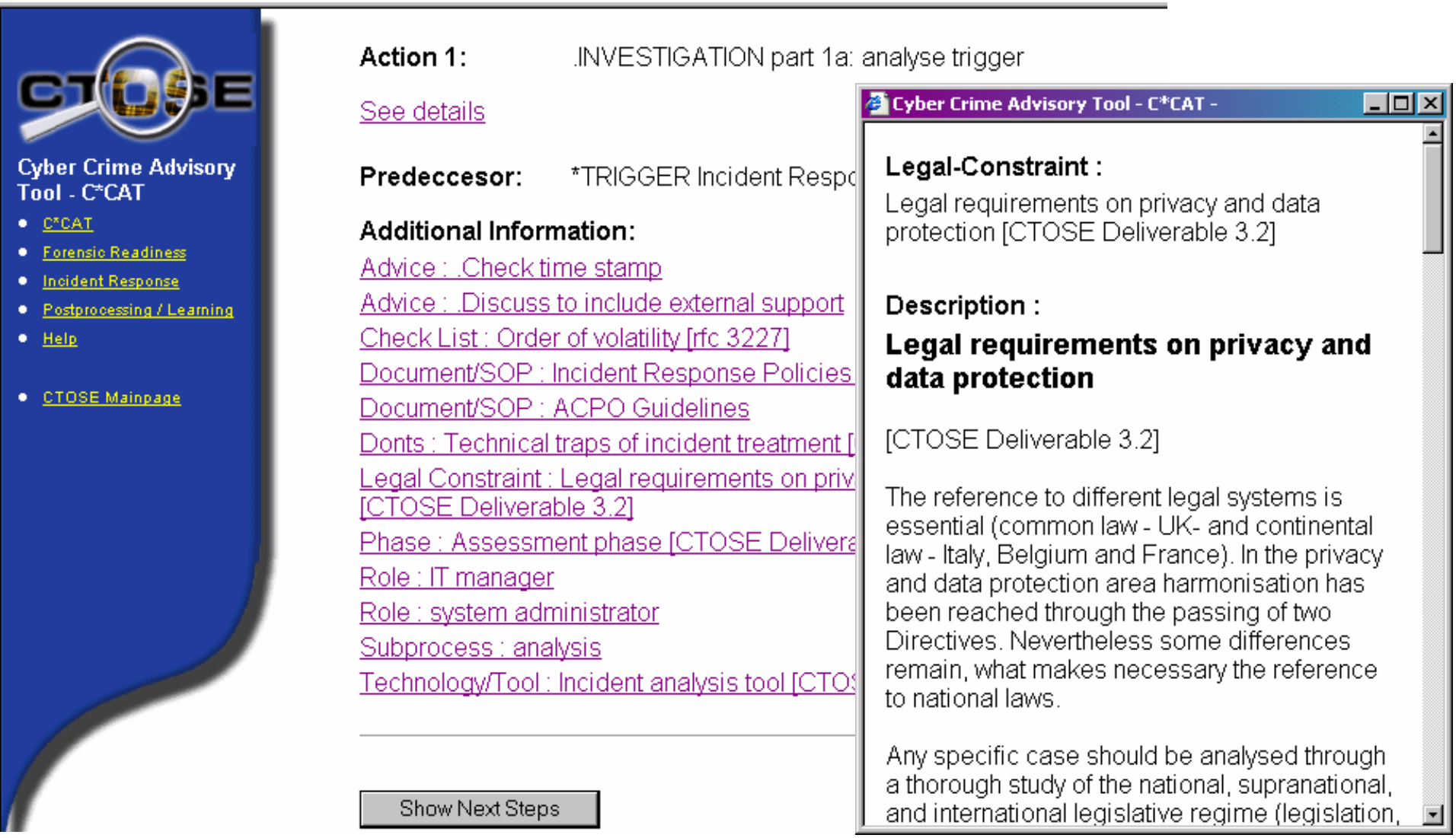
trial?

overall documentation / expert witness /
counter measures / lessons learned

# Prototype Work Flow Management System



# Prototype Work Flow Management System



# The System records...

- which steps taken by whom
- which documents referenced
- which forms filled out
- which person contacted
- which evidence collected and when and by whom

- Result is a virtual container „document“

# Applying the Method

**Preparation phase**

– preparatory measures (risk / threat analysis, cost / benefit analysis, IT security concept, crisis management (business continuity plan, emergency measures, ...), training / awareness, IT security relevant information, IT security tools, technology watch, security audit, etc.)

**Running phase**

– normal state

**Documentation**

– Risks and threats report
– Cost / benefit report
– IT policy and strategy
– **Role model** (definition of responsibilities)
– **Business continuity plan**
– **Emergency plan**
– ...

– Routine measures (**log file** evaluation, updates, etc.)

# Applying the Method

**Investigation phase**

- first analysis of trigger with priority to recover system for normal operation and prevent company image loss
- consolidation meeting - how to proceed?
- key decision: do we want to officially investigate?
- investigation of incident with priority to find out if suspect is internal or external to company
- key decision: is suspect internal or external to company?
- key decision: is »criminal standard of proof« necessary?
- detailed analysis by internal investigator, external investigator or law enforcement
- preparation for court – you never know…

**Documentation**

- **incident report** (form necessary)
  - who, what, where, (how), (why)
- **personal contact with reporter** -> enhance incident report
- Minutes of meeting (decisions, actions, next steps)
- of investigation and outcome
- **of detailed investigation** (forensic, physical, information)
- ...
- -> EXAMPLE

SANS Portal | Create Account

SANS The Most Trusted Source for Computer Security Training

SEARCH

Online Store | Reading Room | Internet Storm Center | GIAC Certification | S.C.O.R.E. | Vendor Opportunities

Free Webcast: September 3, 2003: Six Advanced SSH Techniques

About SANS | Contact SANS | SANS Forum | What's New | F.A.Q. | PGP Key/Local Copy | Surveys | Webcasts

Computer Security News | Research Projects | Computer Security Resources | Sample Policies | Top 20 List

# Sample Incident Handling Forms

## Security Incident Forms

1. Incident Contact List
2. Incident Identification
3. Incident Survey
4. Incident Containment
5. Incident Eradication
6. Incident Communication Log

## Intellectual Property Incident Handling Forms (PDF)

1. Incident Form Checklist
2. Incident Contacts
3. Incident Identification
4. Incident Containment
5. Incident Eradication
6. Incident Communication Log


SANS Web Privacy Policy: www.sans.org/privacy.php
Web Contact:webmaster@sans.org

Feedback

< back to SANS home | Portal Home

printer friendly version >

# Applying the Method

**Investigation phase**

- first analysis of trigger with priority to recover system for normal operation and prevent company image loss
- consolidation meeting - how to proceed?
- key decision: do we want to officially investigate?
- investigation of incident with priority to find out if suspect is internal or external to company
- key decision: is suspect internal or external to company?
- key decision: is »criminal standard of proof« necessary?
- detailed analysis by internal investigator, external investigator or law enforcement
- preparation for court – you never know…

**Documentation**

- **incident report** (form necessary)
  - who, what, where, (how), (why)
- **personal contact with reporter** -> enhance incident report
- Minutes of meeting (decisions, actions, next steps)
- of investigation and outcome
- **of detailed investigation** (forensic, physical, information)
- ...
- -> EXAMPLE

# Example Form for Incident Reporting

**Example**
[http://www.cert.org/reporting/incident_form.txt]:

Your contact and organizational information

- 1. name.....
- 2. organization name.....
- 3. sector type (such as banking, education, energy or public safety.....
- 4. email address.....
- 5. telephone number.....
- 6. other.....

Affected machine(s) (duplicate for each host)

- 7. hostname and IP.....
- 8. time zone.....
  - 9. purpose or function of the host (please be as specific as ossible).....

Source(s) of the attack (duplicate for each host)

- 10. hostname or IP.....
- 11. time zone.....
- 12. been in contact?.....
- 13. Estimated cost of handling incident (if known) .....
- 14. Description of the incident (including dates, methods of intrusion, intruder tools involved, software versions and patch levels, intruder tool output, details of vulnerabilities exploited, source of attack, or any other relevant information): .....

# Applying the Method

**Post Processing Phase**

- final incident analysis and conclusions
- counter measures (IT security)
- evaluation of process model
- if necessary modification of procedure

**Documentation**

- drawn conclusions
- revision of documents within preparation phase
- process evaluation

# Result: Structured Container Document

**Documents**
- Risks and threats report
- Cost / benefit report
- IT policy and strategy
- Role model
- Business continuity plan
- Emergency plan
- Routine measures (log file evaluation, updates, etc.)

**Records**
- incident report personal contact with reporter
- Minutes of meeting (decisions, actions, next steps)
- of investigation and outcome
- of detailed investigation (forensic, physical, information)

**Reports**
- drawn conclusions
- revision of documents
- process evaluation

attributes

attributes

attributes

XML Document

Structured Container Document

# Conclusion: Benefits through Documentation

- having detailed information on incidents
- traceability of incident handling
- prevention of loss of evidence and evidential information
- time and money savings due to general process improvement
- being prepared - having a process in place (incident readiness)
- protection against external accusations
- know-how is documented - not only in head of the experts
- support for quality control - verifiability according to compliance requirements,
- support for validation
- common terminology
- support for investigations which have been internally or externally triggered

# Last Words

**If IT security management (or any other new system)**
**is to be adopted, existing attached business processes should be analysed and optimised ahead of time!**

**Therefore**
- **start at the „beginning“**
- **create a structured, process oriented base for going a practical way**
- **document it and make it transparent**

**and**
- **know the right people and communicate**

# Thank you for your attention!

Sandra Frings
Business Unit Software Management
Fraunhofer-Institute for Industrial Engineering IAO, Stuttgart, Germany
Sandra.Frings@iao.fraunhofer.de
www.sw-management.iao.fhg.de