



Why Good Technology is Necessary, but not Sufficient

IT Risk & Assurance

Mårten Trolin, PhD, CISA

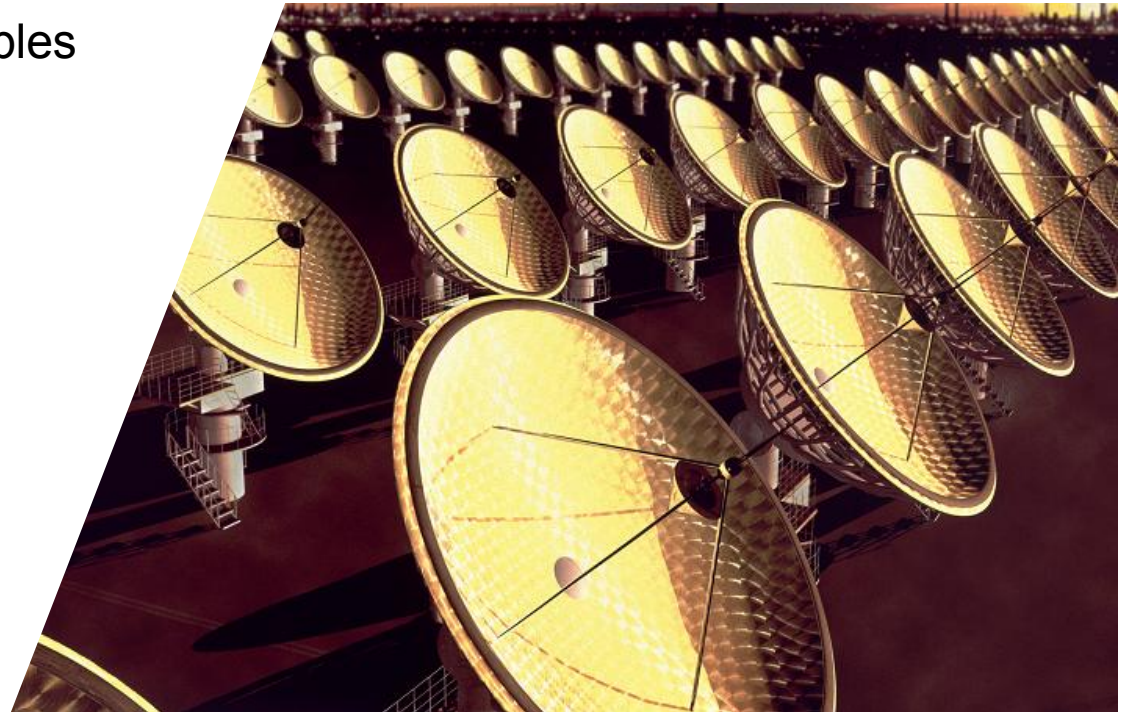
1 December, 2011

Contents

1 Who we are

2 IT Security in practice
- How to build insecure systems from good components

3 Some real-life examples



We are a global knowledge-company with local ties

Approximately 2000 employees with some 70 offices in Sweden
152,000 employees in 140 countries and territories around the globe



Four main business areas

▶ **Assurance**

Audit and qualified accounting issues and accounting

▶ **Advisory services**

Risk management and business development

▶ **Tax**

Tax advice

▶ **Transaction advisory services**

Transaction advice

IT Risk & Assurance

About Ernst & Young

IT Risk and Assurance

Our IT Risk and Assurance professionals help organizations address the challenge of managing IT risks in a way that is in line with their business strategy. We also help our clients and their stakeholders to identify and manage the organization's key IT risks effectively.

▶ Ernst & Young is a global service provider with global methods based on international standards, ensuring a consistent and qualitative approach.



▶ In Sweden we are around 45 IT consultants located in Stockholm, Göteborg and Malmö.

▶ Our consultants are used to working in projects with clear deadlines and maintaining a high quality delivery.

▶ Ernst & Young provides independent auditing and consulting and have no ties to suppliers.

Solution Areas

IT Assurance

We analyze and assess the business management of IT risks. The results are presented in an audit report with improvement proposals, or in a third-party certificate.

IT Controls

We help you to manage business processes and information security in a structured and efficient way through design and implementation of control frameworks.

IT Risk Transformation

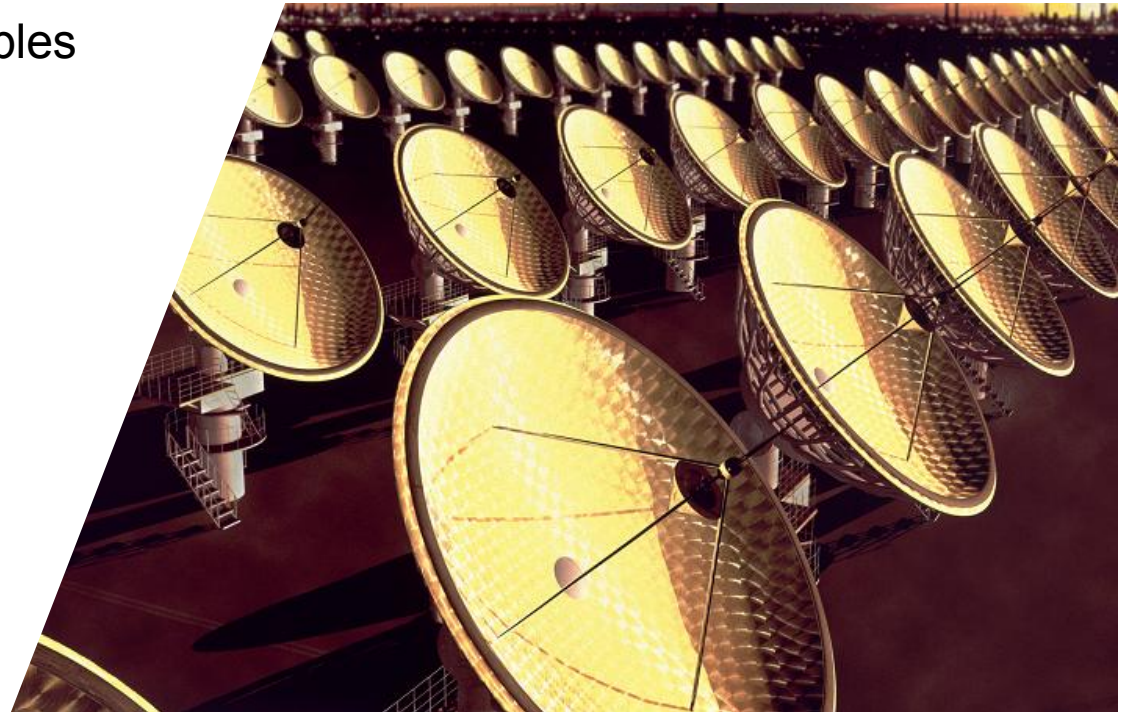
We focus on governing risk in the changing environment of IT, both internally and externally, by advising on IT sourcing demand and follow-up, governance and reporting.

Contents

1 Who we are

2 IT Security in practice
- How to build insecure systems from good components

3 Some real-life examples



IT Security Goals

- ▶ Has the company a clear IT security objective?
- ▶ Is the objective reasonable?
- ▶ Does the company work towards the objective?
 - ▶ Organization
 - ▶ Technology

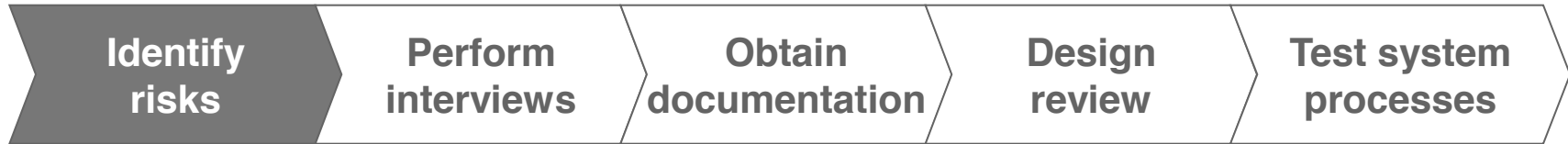


IT Security Audit Method

- ▶ Identify high risk areas
- ▶ Interview employees
- ▶ Get written documentation
- ▶ Analyze the processes (design review)
- ▶ Verify with reality testing
 - ▶ Does the company work according to the descriptions?

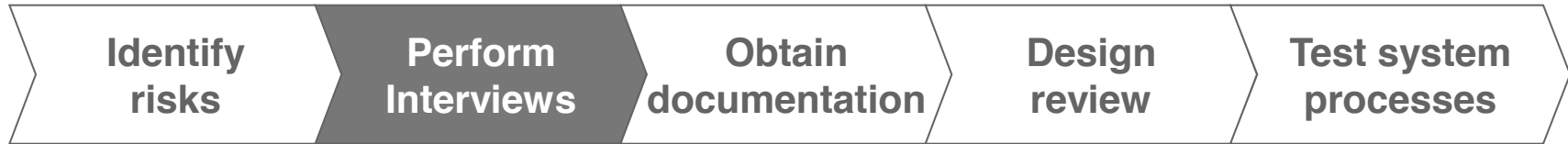


IT Security Audit Method



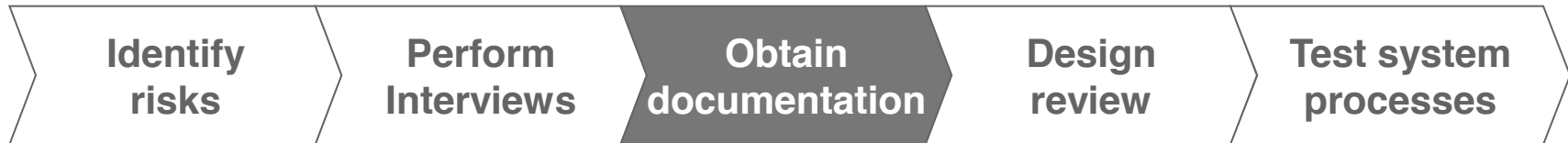
- ▶ Identify high risk areas and (financial) systems, possibly together with financial auditors or the client
- ▶ Assess possible risks
- ▶ Identify significant audit controls
- ▶ Set audit scope
 - ▶ Technical review
 - ▶ Governance review
 - ▶ Process review
 - ▶ Legal compliance review

IT Security Audit Method



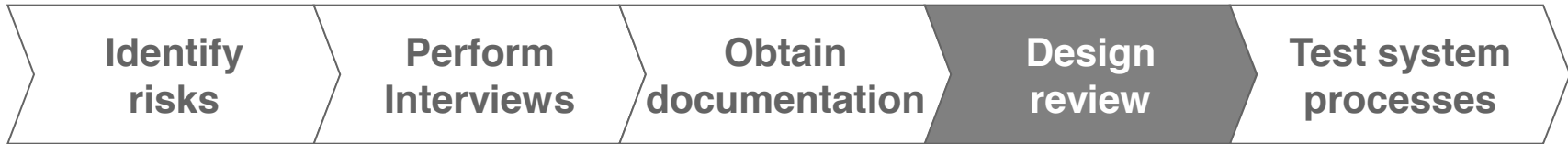
- ▶ Identify and contact responsible personnel
- ▶ Interview personnel working with system input and output
- ▶ Interview systems maintenance and development personnel (servers, DBs, OS & applications)
- ▶ Interview systems administrators
- ▶ If necessary contact (external) systems developer

IT Security Audit Method



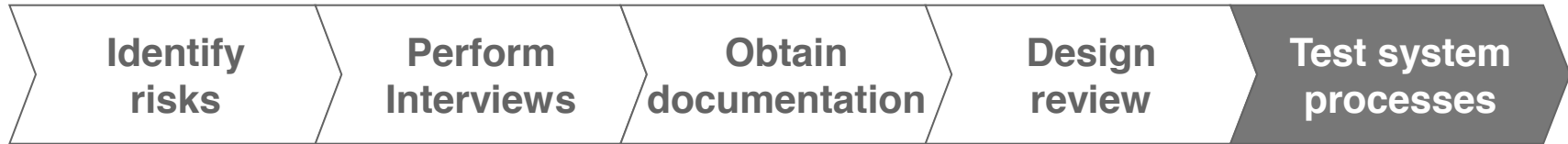
- ▶ Obtain documentation regarding systems and processes in scope
- ▶ Organizational charts
- ▶ Network charts
- ▶ Systems interface charts
- ▶ Flows of data and transactions
- ▶ Changes and problems
- ▶ Process documentation
- ▶ IT policies
- ▶ Operational documentations – system logs, signed documents, authorization lists, personnel lists etc.
- ▶ Risk analyses and continuity planning

IT Security Audit Method



Change Management	Logical Access	IT Operations
<ul style="list-style-type: none"> ▶ Control objectives: Only authorized, tested and approved systems and program changes are implemented in applications, interfaces, databases and operating systems. ▶ Supporting IT General Controls: <ul style="list-style-type: none"> ▶ System and program changes are approved by authorized person ▶ System and software changes are tested ▶ System and program changes have been approved for implementation ▶ Regular follow-ups on implemented changes ▶ Satisfactory separation of duties (SoD) 	<ul style="list-style-type: none"> ▶ Control objectives: Only authorized personnel have access to data and applications to carry out specific functions. ▶ Supporting IT General Controls: <ul style="list-style-type: none"> ▶ General systems and security settings ▶ Password settings ▶ Limited access ▶ Restriction of system recourses and tools ▶ Suitable user permissions ▶ Restricted physical access ▶ Logical access is monitored ▶ Satisfactory separation of duties (SoD) 	<ul style="list-style-type: none"> ▶ Control objectives: Ensure that financial data and information is backed up and can be recomposed with accuracy and completeness. Scheduled jobs are monitored and corrected in time. That incidents are investigated and mitigated in a timely manner. ▶ Supporting IT General Controls: <ul style="list-style-type: none"> ▶ Procedures for backup and restoration of financial data ▶ Deviations from scheduled jobs are identified and resolved within the required time ▶ Problems or incidents in the IT-operations are identified, corrected, examined and analyzed within the required time

IT Security Audit Method



- ▶ Walkthrough and test using the areas in scope
- ▶ For financial audits, the following three categories are covered:
 - ▶ Manage Changes
 - ▶ Logical Access
 - ▶ IT Operations
- ▶ Test samples are taken for each area and reviewed
- ▶ If mistakes are detected, mitigating controls are investigated in order to evaluate the risk

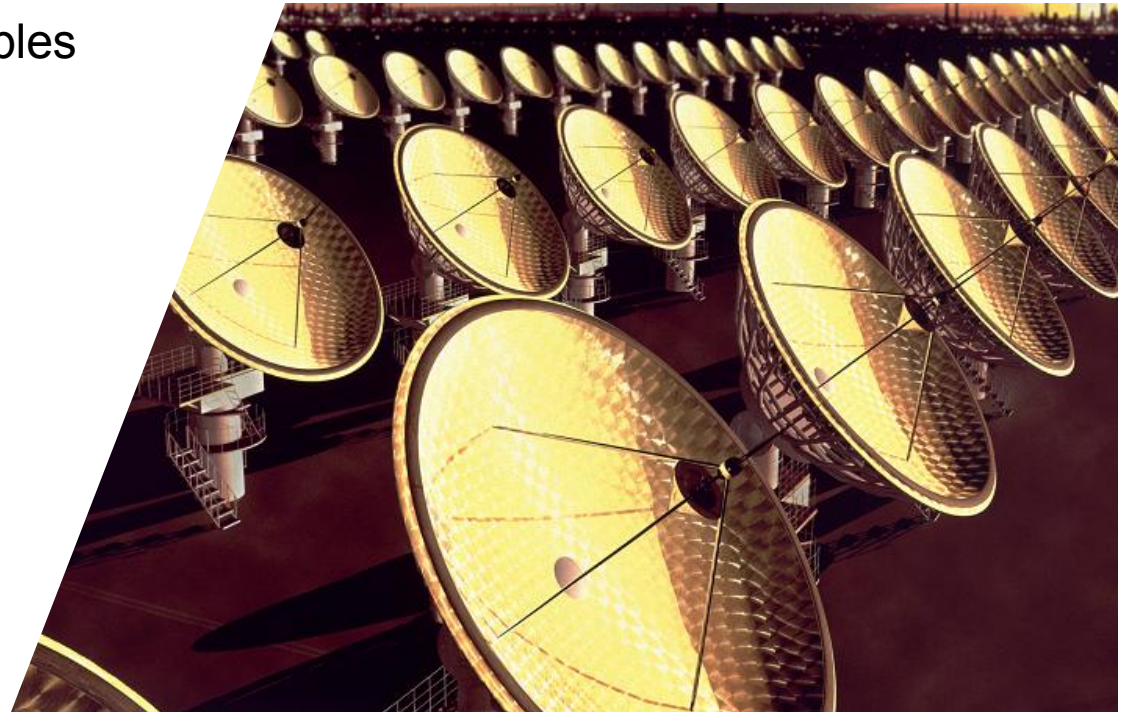


Contents

1 Who we are

2 IT Security in practice
- How to build insecure systems from good components

3 Some real-life examples



Lack of Formalized Procedures

“We don’t need to write this down”

“We are too busy to spend time writing papers”

“No-one would read it anyway”

Non-Compliance with Formal Procedures

“Are there rules?”

“The procedures are too complicated.”

“You know, that doesn’t apply to me, because...”

“No-one cares if we do it by the book or not.”

Lack of Segregation of Duties

“It is not a problem in our company, because...”

“Our IT department is too small”

“Why would we need that?”

Lack of Traceability

“It is so much easier to use the same account for everyone.”

“We log everything and store it a secure folder on the server.”

“We log everything, but we need to clear the log every week to save disk space.”

“We usually log everything, but we had to turn it off last month.”

Lack of Test Procedures

“It is quite enough to test the new functions.”

“It is too expensive to build a separate test environment.”

“We just make sure to monitor the application carefully after putting it into production.”

Lack of Good Access Management

“Paper-work for every user is just a waste of time.”

“It is the responsibility of the immediate supervisor to inform us when privileges are to be removed.”

“To save time, we copy the access rights of an existing user.”

No Tests of Backup Tapes

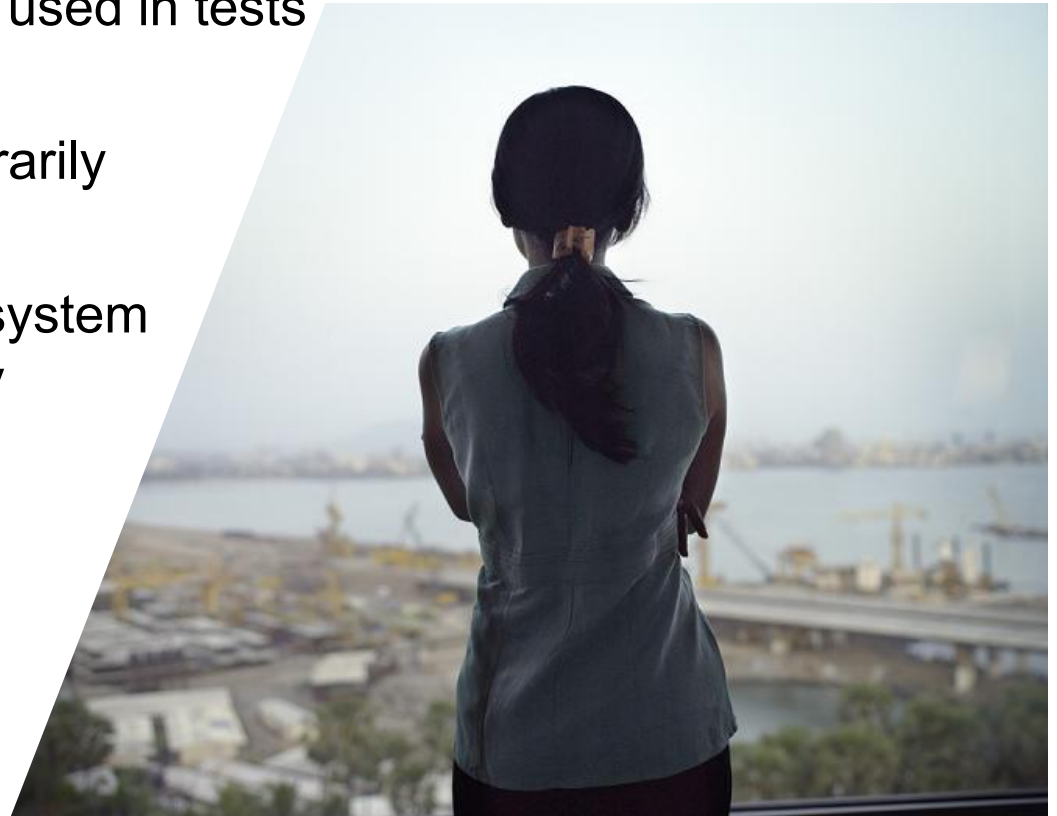
“We don’t need to, because our system cannot produce invalid backups.”

“We do it once every month, except that extraordinary circumstances prevented us from testing the last three months.”

“That is the responsibility of the XYZ department.”

Real-Life Examples

- ▶ Password in drawer or under keyboard
- ▶ Sensitive production data used in tests
- ▶ Firewall rules added arbitrarily
- ▶ Users not removed from system after leaving the company



Who Does the Job

IT Security

- ▶ Specialized IT security personnel, CISO, CSO CIO etc.

Internal audit

- ▶ The organizations own internal audit (usually larger companies and government authorities).

External audit

- ▶ As a part of the external audit

IT Personnel

- ▶ Non-specialized IT personnel (usually MSEs)

Consultants

- ▶ Performing a complete IT-audit or supporting above mentioned parties in different ways



www.ey.com/se

The information contained within this document and any related oral presentation conducted by Ernst & Young AB (EY) contains proprietary information and may not be disclosed, used or duplicated - in whole or in part - for any purpose without the express written consent of EY.

 ERNST & YOUNG
Quality In Everything We Do