چند رسانه ای
نگارستان

سمینار آموزشی سیستم مدیریت امنیت اطلاعات
بر پایه سیاستهای استانداردهای
BS7799 & BS15000

سمینار آموزشی چهارم

Part Four

BS7799-2 Certification Process

INFORMATION SECURITY MANAGEMENT SYSTEM

Houman Sadeghi Kaji
Spread Spectrum Communication System PhD. ,
Cisco Certified Network Professional Security Specialist
BS7799 LA
info@houmankaji.net

Agenda

- **ISMS Certification Audits**
  - Certify?
  - Structure of BS7799 certification
  - Auditing(Audit methodology)
  - BS7799-2 Certification Why and How?(Assessment)
  - How much it costs?
  - Report audit results
  - Corrective Action/Follow up(Certification decision)
  - ISMS Scope of certification
  - Surveillance and Recertification audits

Questions

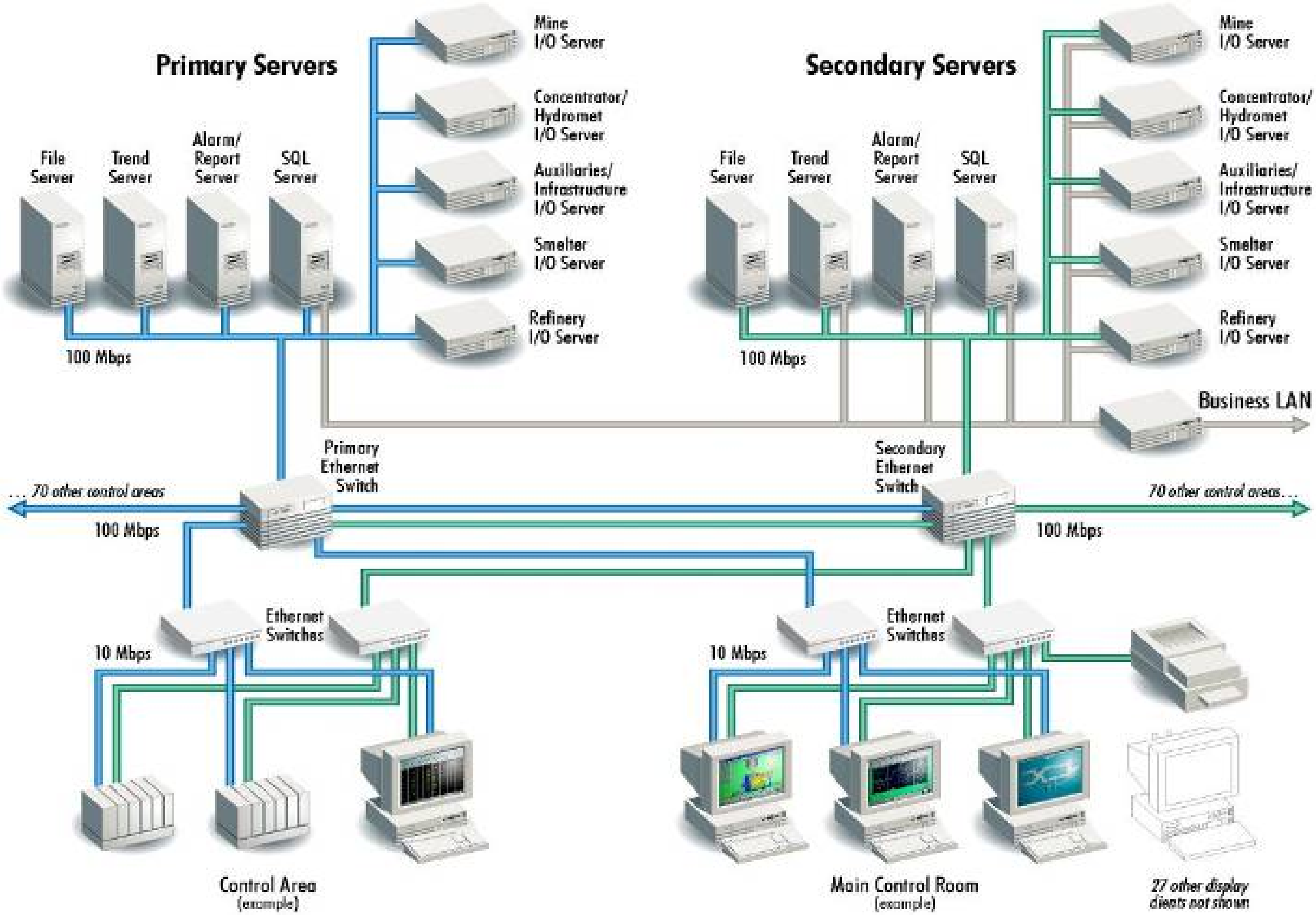
- Do you protect all your company assets?

Questions

- Do you know all risks relating to your processes and business continuity?

Questions

- Do you know a systematic way to tackle with attacks to your complex systems?



Questions

- How reliable are your solution in this battle?

Business is a world of Managing Risks

Maritime industry

Renewable energy sector

Food and beverage

Aviation

Oil and gas industry

Managing risk

ICT

Process industry

Automotive

Rail industry

General

Structure of BS7799 certification

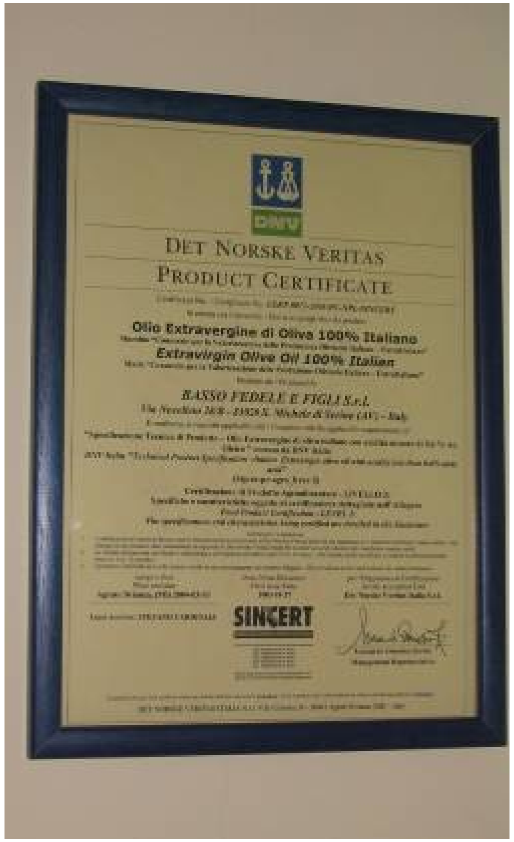
INFORMATION SECURITY
MANAGEMENT SYSTEM

Certification

- **Certify:**

to state (something) officially, usually in writing, esp. that (something) is true or correct

(from Cambridge International Dictionary of English)



DNV

DET NORSKE VERITAS
PRODUCT CERTIFICATE

[illegible]

Olio Extravergine di Oliva 100% Italiano

[illegible]

Extravirgin Olive Oil 100% Italian

[illegible]

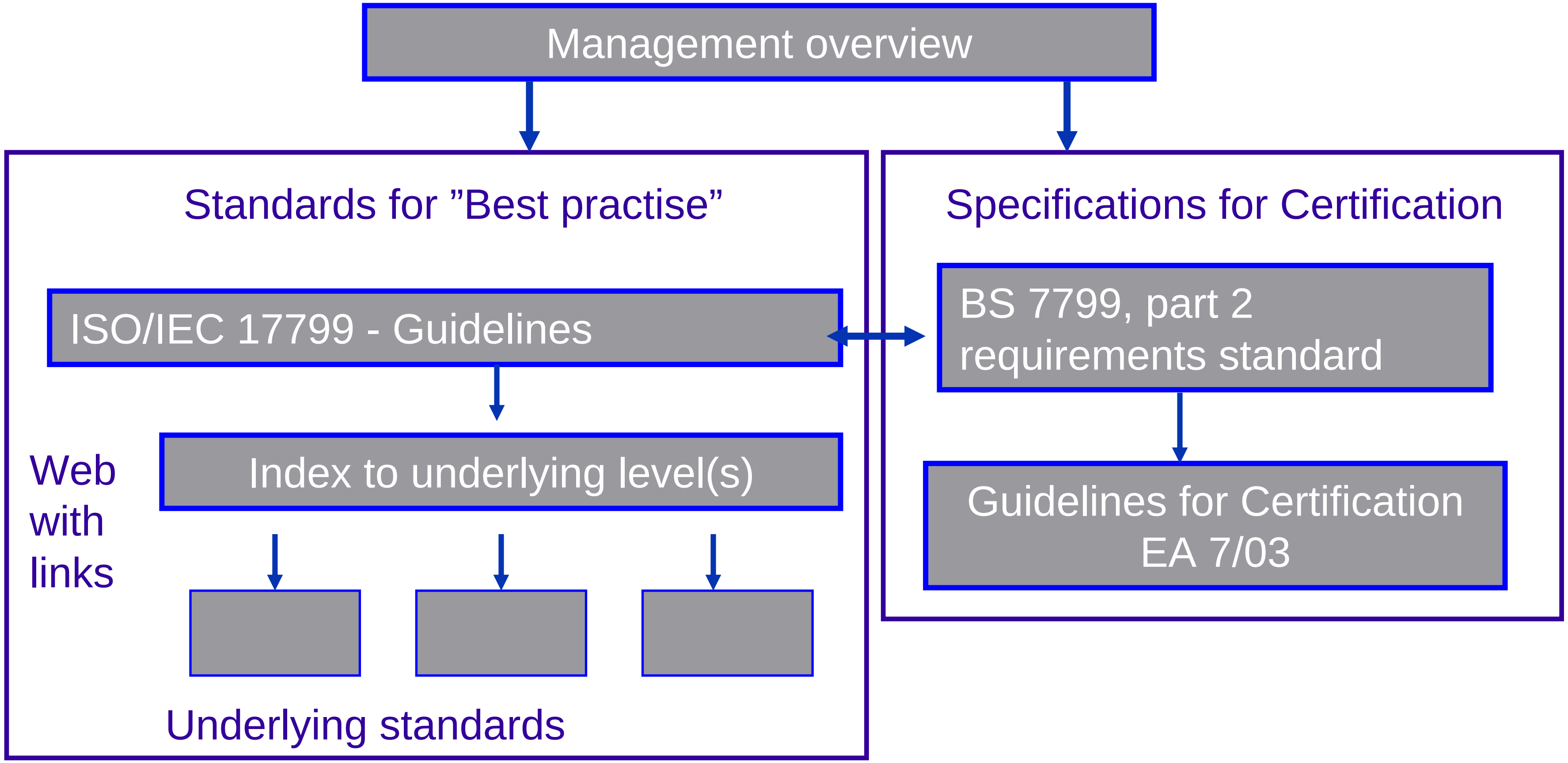
BASSO FEDELE E FIGLI S.r.l.

Via Nevellino 36/R - 83028 S. Michele di Serino (AV) - Italy

[illegible]

SINCERT

Structure



Management overview

Standards for "Best practise"

ISO/IEC 17799 - Guidelines

Web with links

Index to underlying level(s)

Underlying standards

Specifications for Certification

BS 7799, part 2 requirements standard

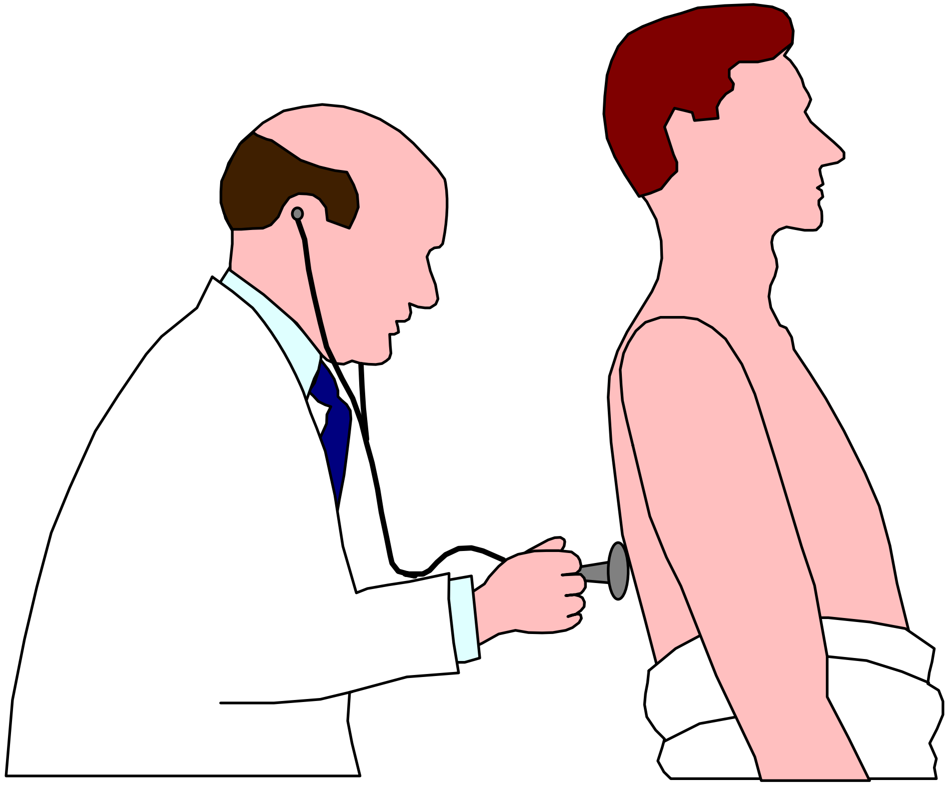
Guidelines for Certification EA 7/03

Auditing

INFORMATION **S**ECURITY
MANAGEMENT **S**YSTEM

WHAT IS AN AUDIT?

- A health check
- Key words
  - Systematic
  - Documented
  - Periodic
  - Objective
  - Verification



KEY CONCEPTS

Systematic	Carried out in accordance to set protocols
Documented	Reports are prepared
Periodic	Conducted to established schedule
Objective	Auditors have some independence
Verification	Evaluate compliance to requirements

What is an Audit?

3.9.1 audit

- systematic, independent and documented **process** (3.4.1) for obtaining **audit evidence** (3.9.4) and evaluating it objectively to determine the extent to which **audit criteria** (3.9.3) are fulfilled.

WHY AUDIT?

- Determine Information Security system effectiveness
- Identify existing nonconformities
- Highlight areas of strength
- Point out areas for improvement
- Identify requirements for corrective and/or preventive action

SUMMARY - KEY QUESTIONS

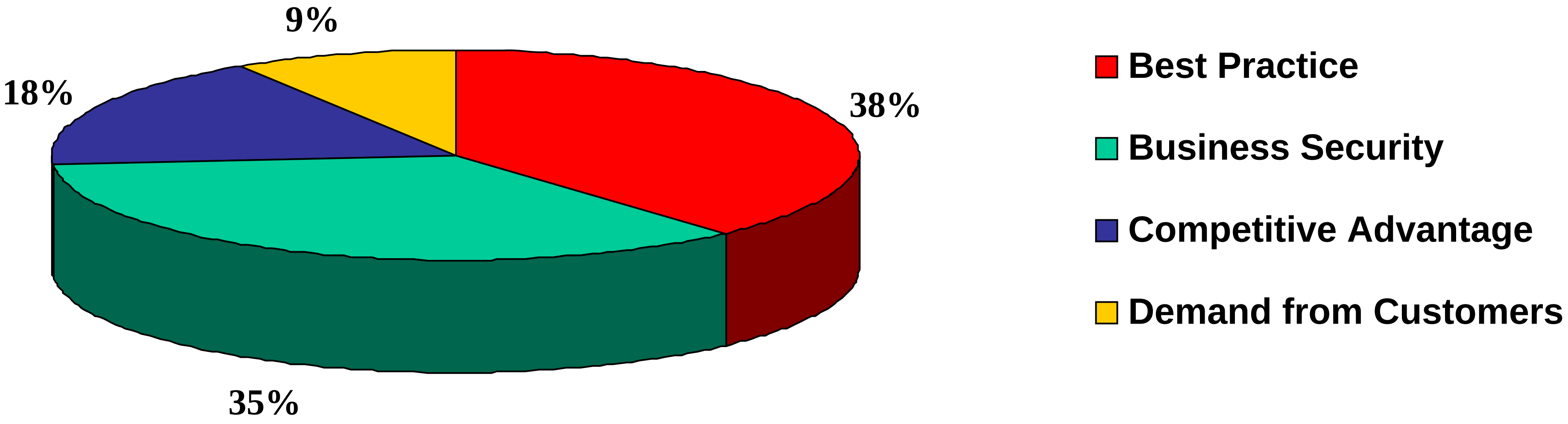
- Is ISMS based on identification/evaluation of risks?
- Are there procedures to address all clauses of standard?
- Is system being implemented consistently and systematically?
- Does the ISMS deliver performance improvement and regulatory compliance?

BS7799-2 Certification Why and How?

INFORMATION **S**ECURITY
MANAGEMENT **S**YSTEM

Reasons for seeking Certification

BSI-DISC survey 1999 in co-operation with Admiral Plc.



Other reasons quoted for seeking Certification include:
“To show compliance with the new Data Protection Act”
“To be able to request compliance from other organisations”
“To facilitate compliance with best practice framework”

Path to Certification

BS 7799 CERTIFICATION

RECCOMENDATION FOR CERTIFICATION

EXTERNAL REVIEW

FIXING NON-CONFORMANCES

INTERNAL AUDIT AND REVIEW

IMPLEMENTING SECURITY POLICY

RISK ASSESSMENT	RISK ASSESSMENT REPORT	BS7799 CONTROL DOCUMENT	SCOPE OF POLICY DOCUMENT	PREPARING THE POLICY DOCUMENT	MAPPING BS 7799 DOMAINS TO POLICY DOCUMENT	STATEMENT OF APPLICABILITY

Developing ISMS

»Review of Documentation

»Selecting Team for Internal Audit

»Training for Users

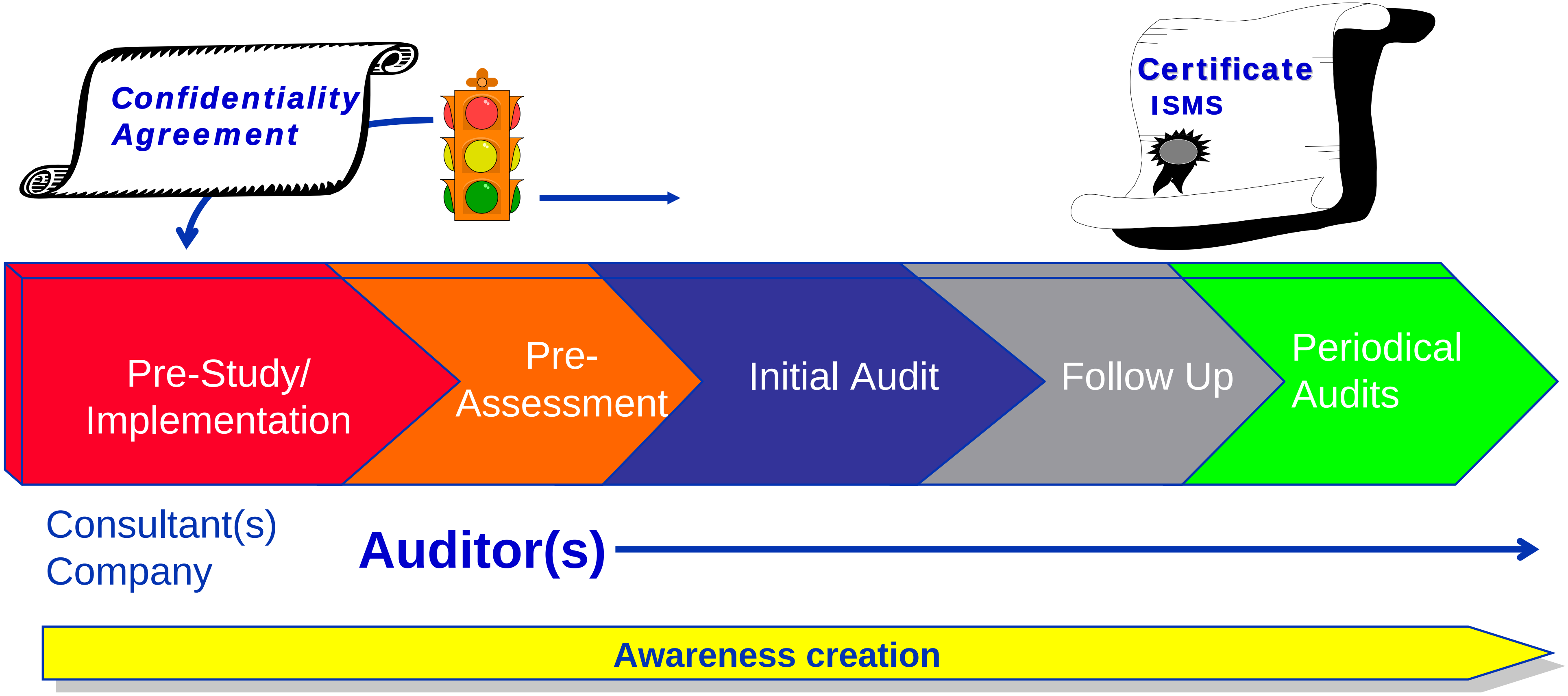
»Conducting Internal Audit

»Finding Non-Conformances

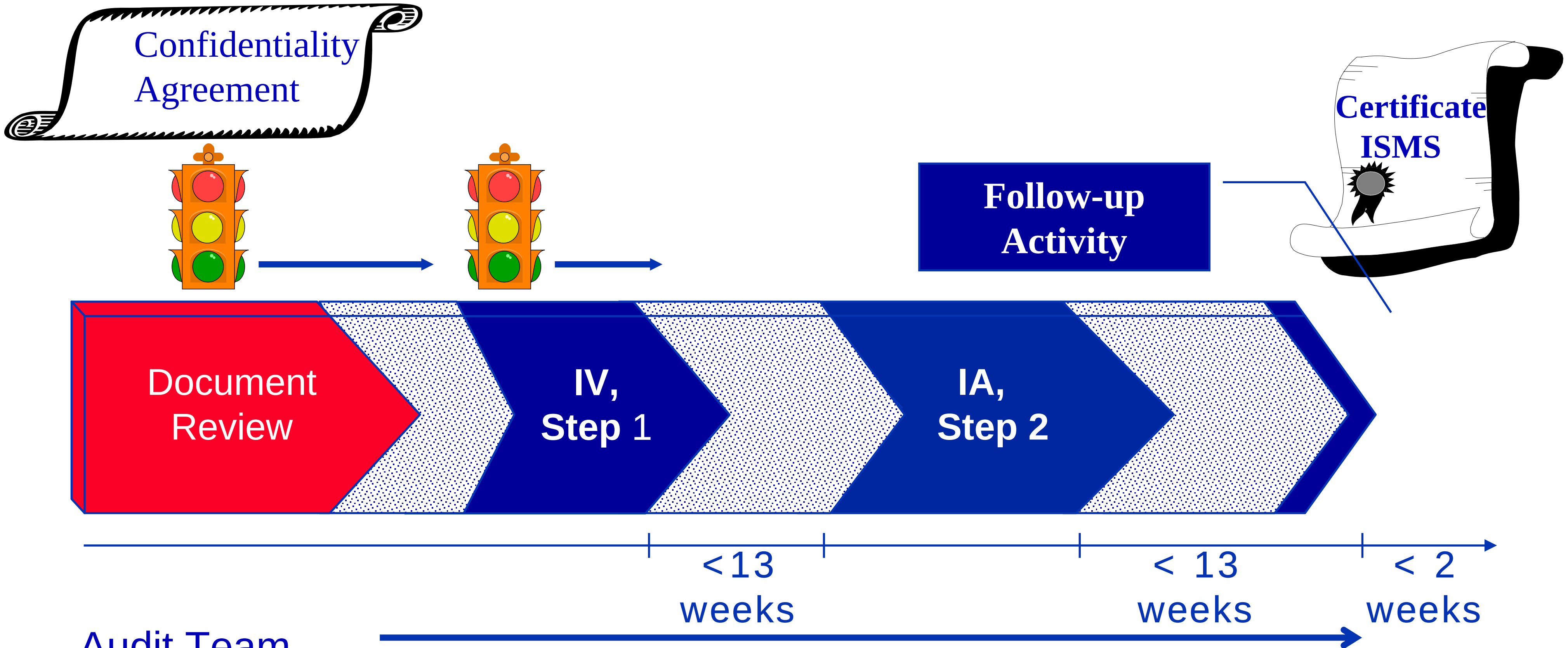
»Fixing Non-Conformances

»Final Management Review

When can certification take place?



Initial Audit Process

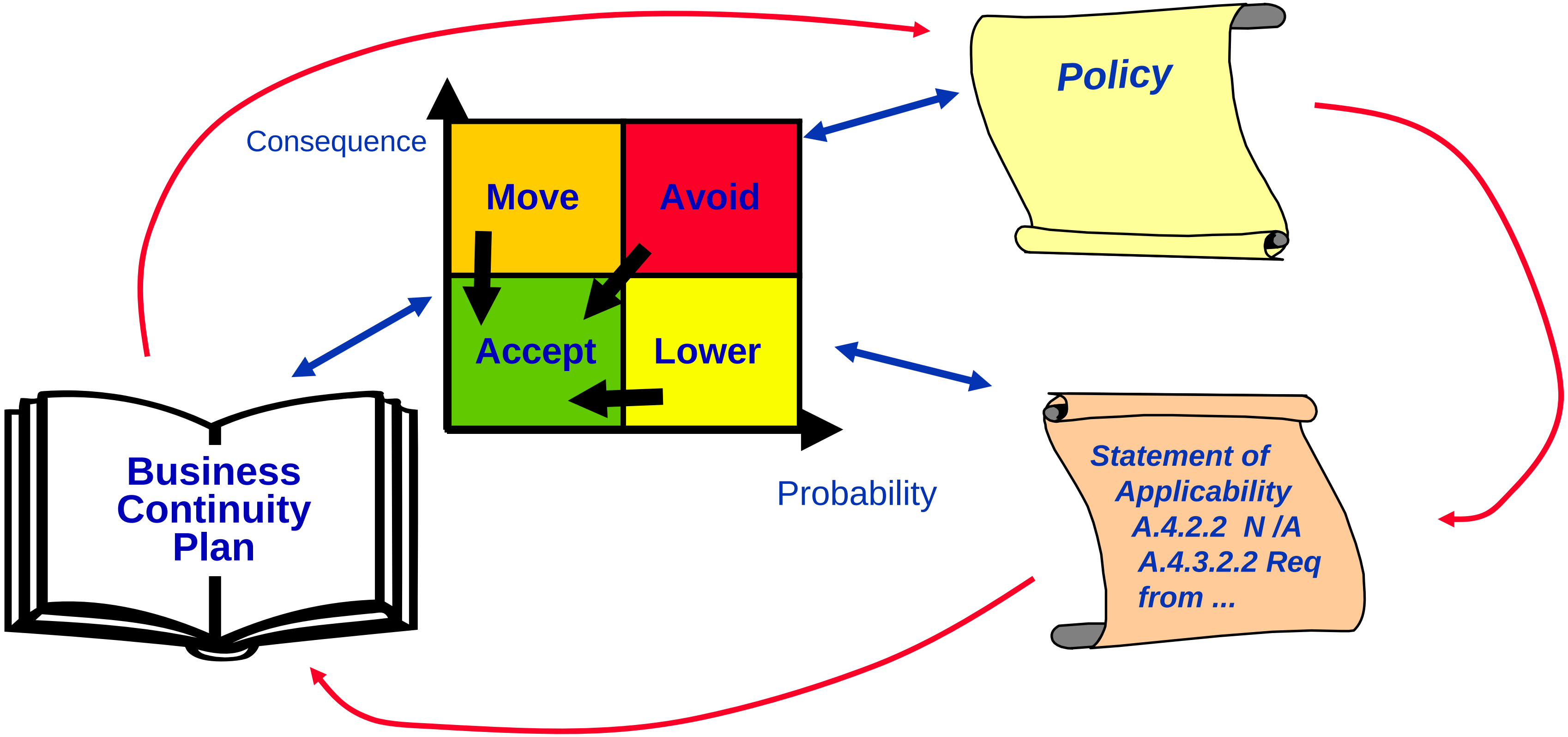


Audit Team,
Incl. Technical Expert

Steps in the initial audit process

Document review	Step 1 (IV)	Step 2 (IA)
▪ System documentation ISMS ▪ Policy ▪ Scope ▪ IT-environment documentation ▪ Statement of Applicability ▪ Risk analysis ▪ Business Continuity Plan	▪ Presentation of the report from the document review ▪ Initial technical evaluation	▪ Presentation of the report from Step 1 ▪ Implementation of ISMS to be evaluated ▪ Validation of conformance with requirements
Result ▪ Report	**Result** ▪ Report ▪ Non-conformities, to be closed before Step 2 is initiated	**Result** ▪ Report ▪ Non-conformities, to be closed before the certificate is handed out ▪ Recommendation to Certification

The risk Assessment is the focal point



What happens during a certification audit, 1?

Records available?

- Risk Analysis/Assessment
- Business Continuity Plan
- Policy
- Statement of Applicability

- Correct and relevant?
- Known and tested?
- Communicated?

What happens during a certification audit, 2?

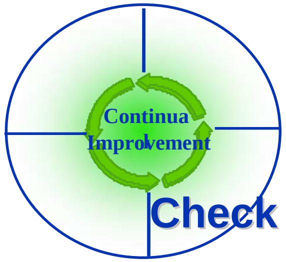
Records available?

- Security in job definition and resourcing
- User training
- Virus control
- Protection of important acts and registers
- Data protection

- Implemented?

What happens during a certification audit, 3?

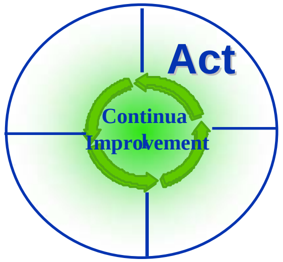
- Incident reporting
- Software copyright compliance
- Compliance with legal requirements
- Technical Compliance



- **Records available?**

- Regular controls?
- Followed up?
- Preventive actions identified?

What happens during a certification audit, 4?



- **Records available?**

MANAGEMENT REVIEW

- Regularity of meetings?
- Commitment shown?
- Improvement suggestions?

Security policy

BS 7799-2:2002, Annex A

The auditor verifies:

- Management commitment
- That the security policy is known
- Compliance

- Provide direction
- Show commitment

Random samples and objective judgement

Statement of Applicability from an audit point of view

A.4.2.2 N/A
A.4.3.2.2 Req from ...

The auditor verifies:

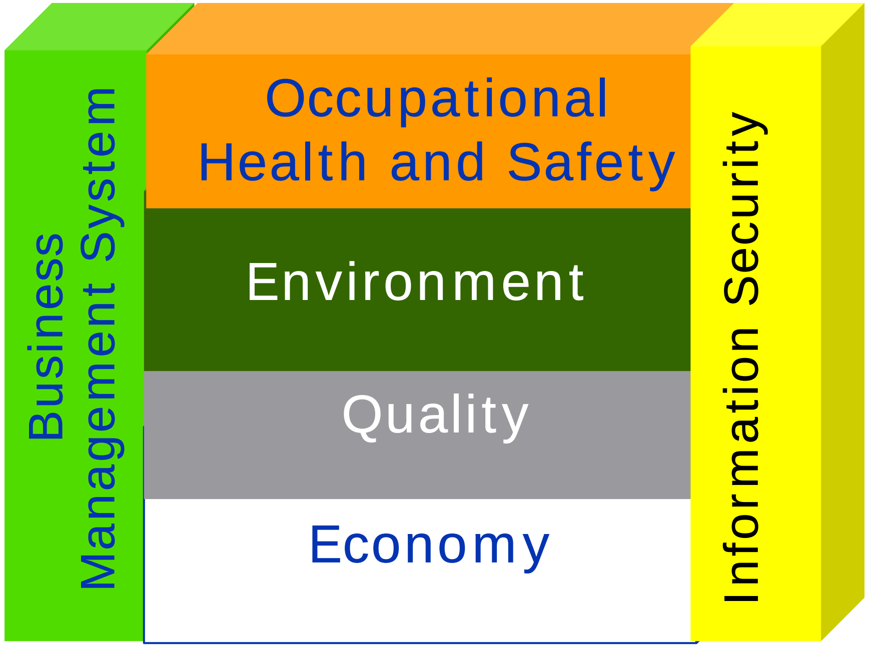
- How the implementation of controls and control objectives are conformed to within the organisation
- Selections made

The auditor evaluates:

- The risk analysis
- The security level

Random samples and objective judgement

Co-ordination with other audits



- Quality Management System
- Environmental Management System
- Occupational Health and Safety Management System
- Information Security Management System

A SINGLE BUSINESS MANAGEMENT SYSTEM Audit TEAM

Certification of ISMS will

- Heighten security awareness within the organisation
- Identify weak parts in the Business Risk Assessment
- Improve the structure for continuous improvement
- Improve the system
- Be a confidence factor internally as well as externally
- Enhance the knowledge and importance of security-related issues at the management level
- Ensure that ”knowledge capital” will be ”stored” in a business management system
- Enable future demands from clients, stockholders and partners to be met

How much it costs?

INFORMATION **S**ECURITY
MANAGEMENT **S**YSTEM

Cost of an initial certification

Depends on:

- The size of the company
- Scope
- Impacting factors (business activity/company structure)
- IT-structure (size and complexity)
- The readiness for certification within the company
- Prior certification

~ £10,000 for a company with 100 employees provided medium impacting factors and medium size and complex IT-structure.

Reporting audit results

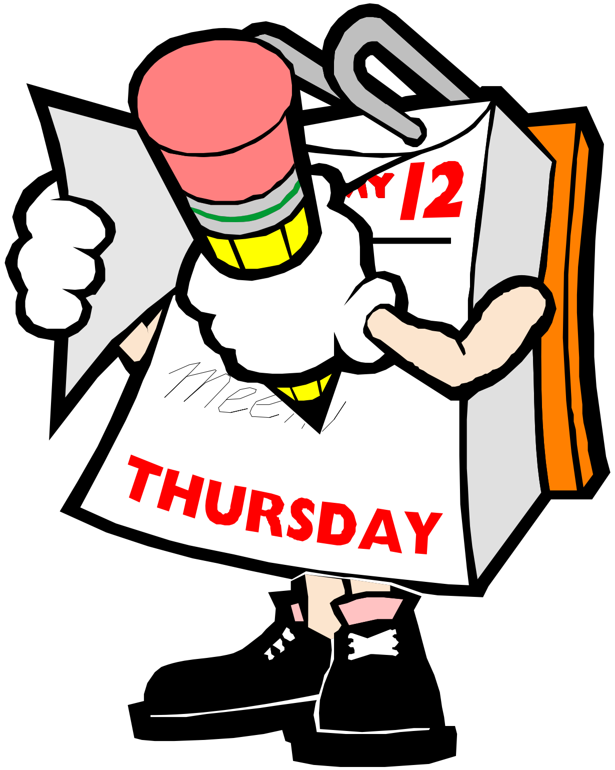
INFORMATION **S**ECURITY
MANAGEMENT **S**YSTEM

The Audit Report

- Provides summary of audit results
- No surprises
- Formal record
- Lead Auditor is responsible

Contents of Audit Report

- Purpose of audit
- Date
- Audit team
- Scope/areas covered
- Key contacts
- Information Management System documents
- Summary statement
- Areas for improvement
- Action items
- **Appendices**
- Completed checklist
- Copies of Corrective Action Requests (nonconformities) submitted for auditee response
- Follow-up schedule



Corrective Action/Follow up (Certification decision)

INFORMATION **S**ECURITY
MANAGEMENT **S**YSTEM

Corrective Action/Follow-up

Key Points:

- Reviewing corrective action responses
- Conducting effective follow-up audits

RESPONSIBILITIES

"The auditee is responsible for determining and initiating corrective action needed to correct a nonconformity or to correct the cause of a nonconformity.

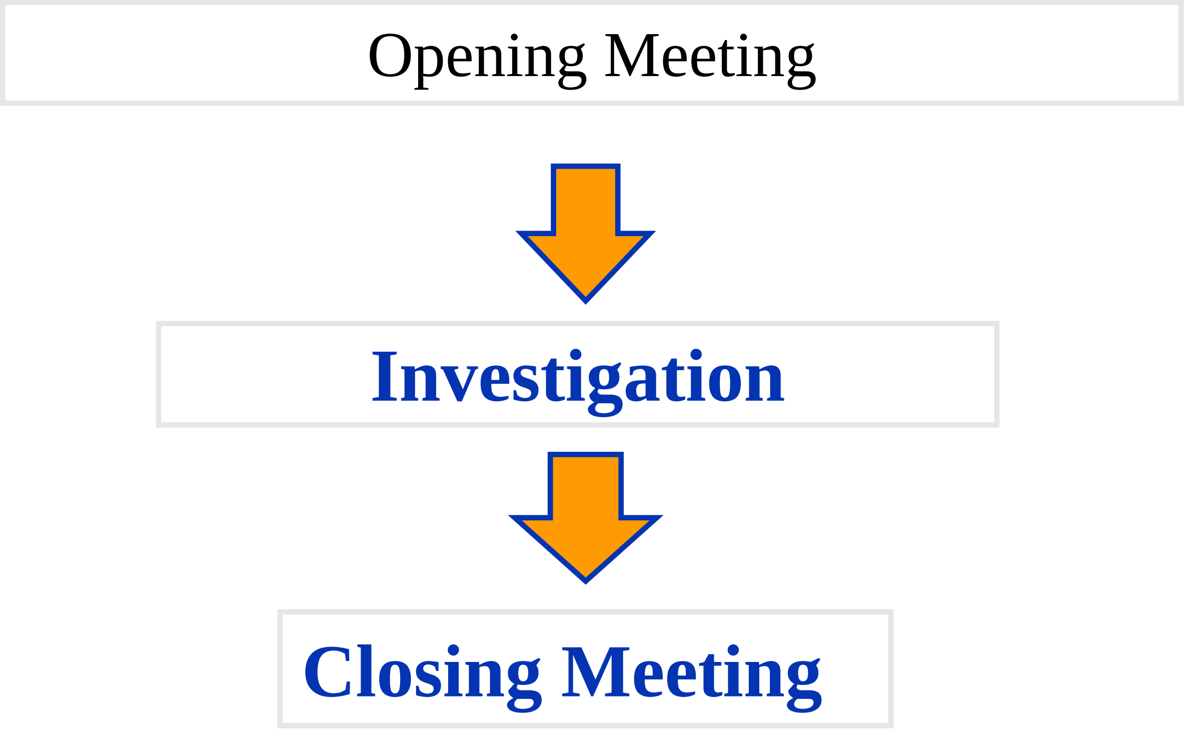
The auditor is only responsible for identifying the nonconformity."

ISO 19011

If Corrective Action is Inadequate ...

- **Follow audit procedures**
- **Escalate to management for review, if required**

FOLLOW-UP VISITS



Opening Meeting

Investigation

Closing Meeting

Scope of certification

INFORMATION **S**ECURITY
MANAGEMENT **S**YSTEM

IS8 - Scope of certification

- The organisation should define **the scope** of the Information Security Management System (ISMS)
- Interfaces/delimitations should be identified and included in the risk assessment; i.e. ”shared site”
- The certification body shall secure that **the risk assessments** are **relevant** and **mirror the business area** for the chosen scope

EA 7/03

Surveillance and Recertification

INFORMATION **S**ECURITY
MANAGEMENT **S**YSTEM

Surveillance and Recertification audits

- Surveillance audits at yearly basis
  - semi-annual, every nine months or once a year
- Audit methodology - the same as during a certification audit
- Surveillance audits may be combined with audits of other management systems whereby the complete business management system is audited at the same time
- Reassessment after 3 years…

A reference to start with

- http://www.xisec.com/faqs.htm
- http://www.bs15000.org.uk

Question

- Do you protect all your company assets?