ISO 27001 Implementation

Presented to:
ISACA

March 24, 2016

Presenters:

- Russ Walsh – GRC21 - Managing Partner
- Jim Macellaro – Jim Macellaro Consulting - Founder

Agenda

- ISO 27000 Overview
- The ISMS
- Planning the Implementation
- Deploying the ISMS
- Measurement and Continual Improvement

ISO 27000 OVERVIEW

Audience

- Certifications:
  - CISA
  - CISSP
  - ISO 27001
    - Which version – 2005 or 2013
- Reason for attending
  - Industry
    - Planning for ISO 27001
    - Expanding ISO 27001
    - General knowledge
  - Consulting
    - Building or expanding ISO 27001
    - Certification firms

ISO Management Principles

Customer Focus

Leadership

Involvement of People

Process Approach

System Approach to Management

Continual Improvement

Factual Approach to Decision Making

Mutually Beneficial Supplier Relationships

The Standards

- ISO
  - 19,000 standards since 1947

- ISO 27000
- ISO 27001
- ISO 27002
- ISO 27003
- ISO 27004
- ISO 27005
- ISO 31000

- 14 clauses, 35 control objectives, 114 controls

Terminology (lingo)

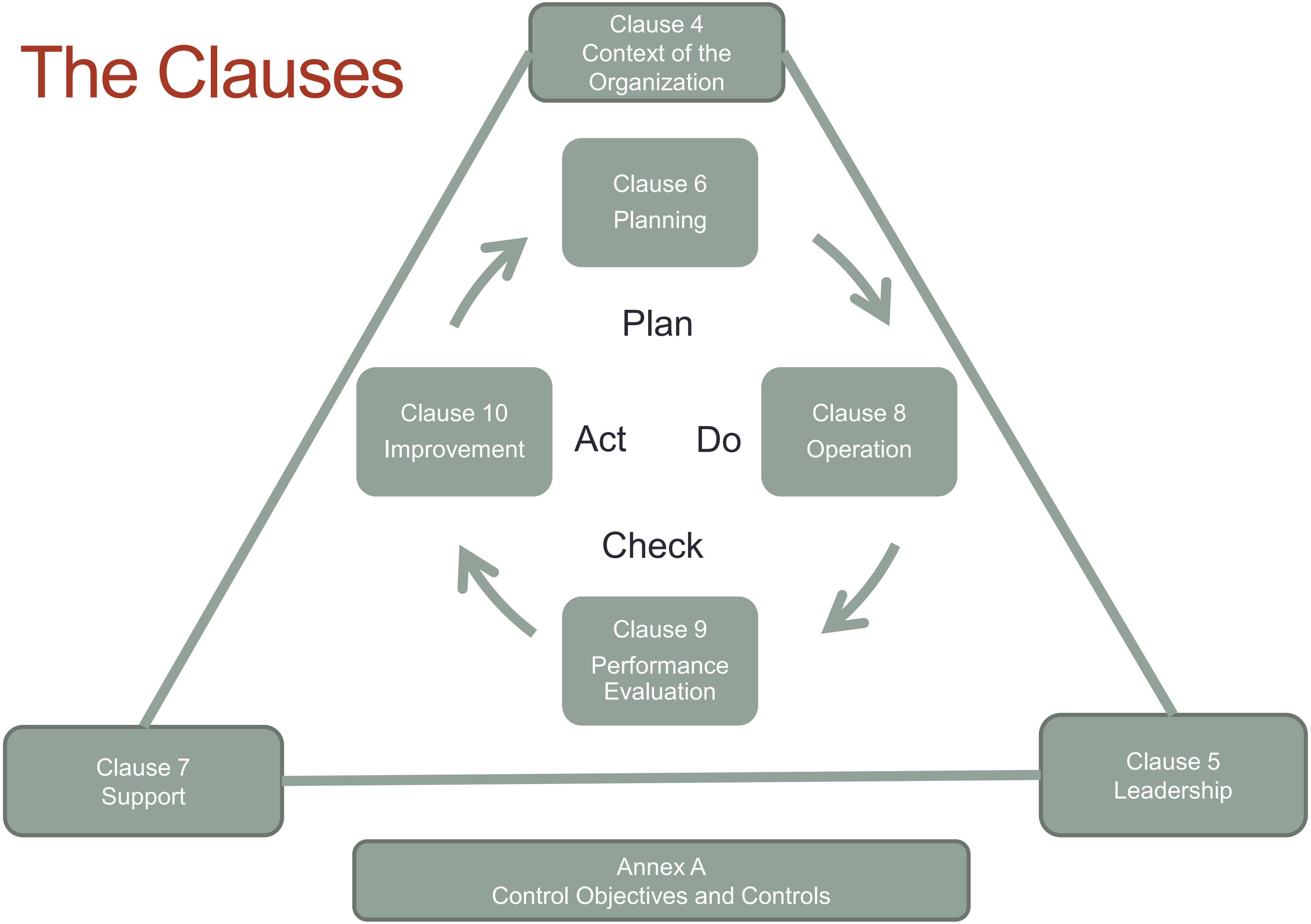
- SOX
  - Interim testing, roll forward testing, significant deficiencies, material weaknesses
  - Final report issued by external auditors (typically the Big 4)
- SOC 1/2
  - Gaps, observations, recommendations
  - SOC report – generally issued by a CPA firm
  - ITGC / Domains
- PCI
  - Final report is called a ROC (report of compliance) – generally issued by an InfoSec Compliance firm
- ISO 27001
  - Stage 1, Stage 2, Surveillance Audits
  - Certification – only a few firms do this

THE ISMS

Definition of ISMS

- An Information Security Management System consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.
- An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.
- It is based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks.

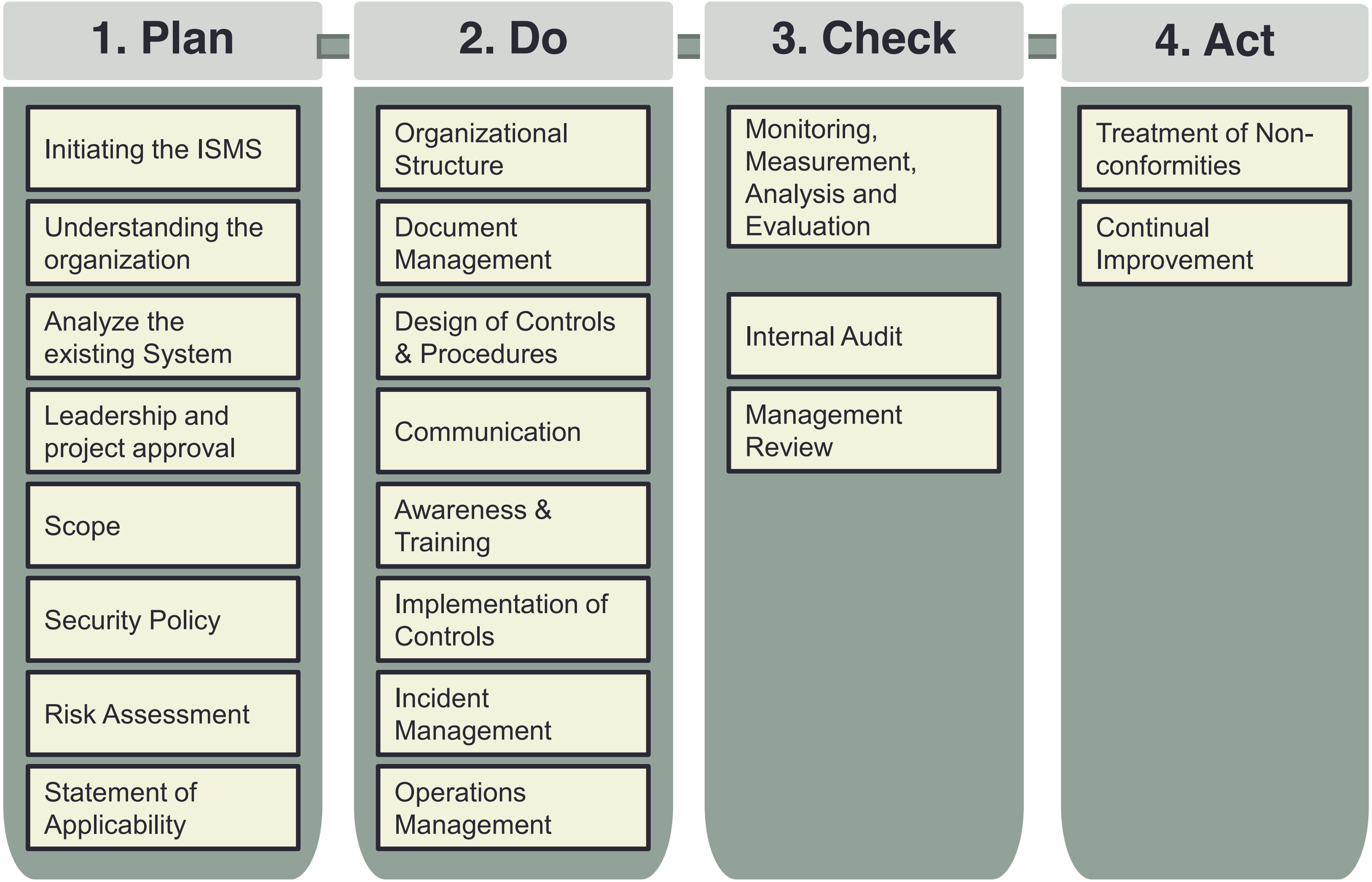
The Clauses


Clause 4
Context of the Organization
Clause 6
Planning
Plan
Clause 10
Improvement
Act
Do
Clause 8
Operation
Check
Clause 9
Performance Evaluation
Clause 7
Support
Clause 5
Leadership
Annex A
Control Objectives and Controls

ISO 27002 Clauses

		Nbr of Controls
5	Information Security Policies	2
6	Organization of Information Security	7
7	Human Resources	6
8	Asset Management	10
9	Access Control	14
10	Cryptography	2
11	Physical And Environmental Security	15
12	Operations Security	14
13	Communications Security	7
14	System Acquisition, Development And Maintenance	13
15	Supplier Relationships	5
16	Information Security Incident Management	7
17	Information Security Aspects Of Business Continuity Management	4
18	Compliance	8

Framework



1. Plan

- Initiating the ISMS
- Understanding the organization
- Analyze the existing System
- Leadership and project approval
- Scope
- Security Policy
- Risk Assessment
- Statement of Applicability

2. Do

- Organizational Structure
- Document Management
- Design of Controls & Procedures
- Communication
- Awareness & Training
- Implementation of Controls
- Incident Management
- Operations Management

3. Check

- Monitoring, Measurement, Analysis and Evaluation
- Internal Audit
- Management Review

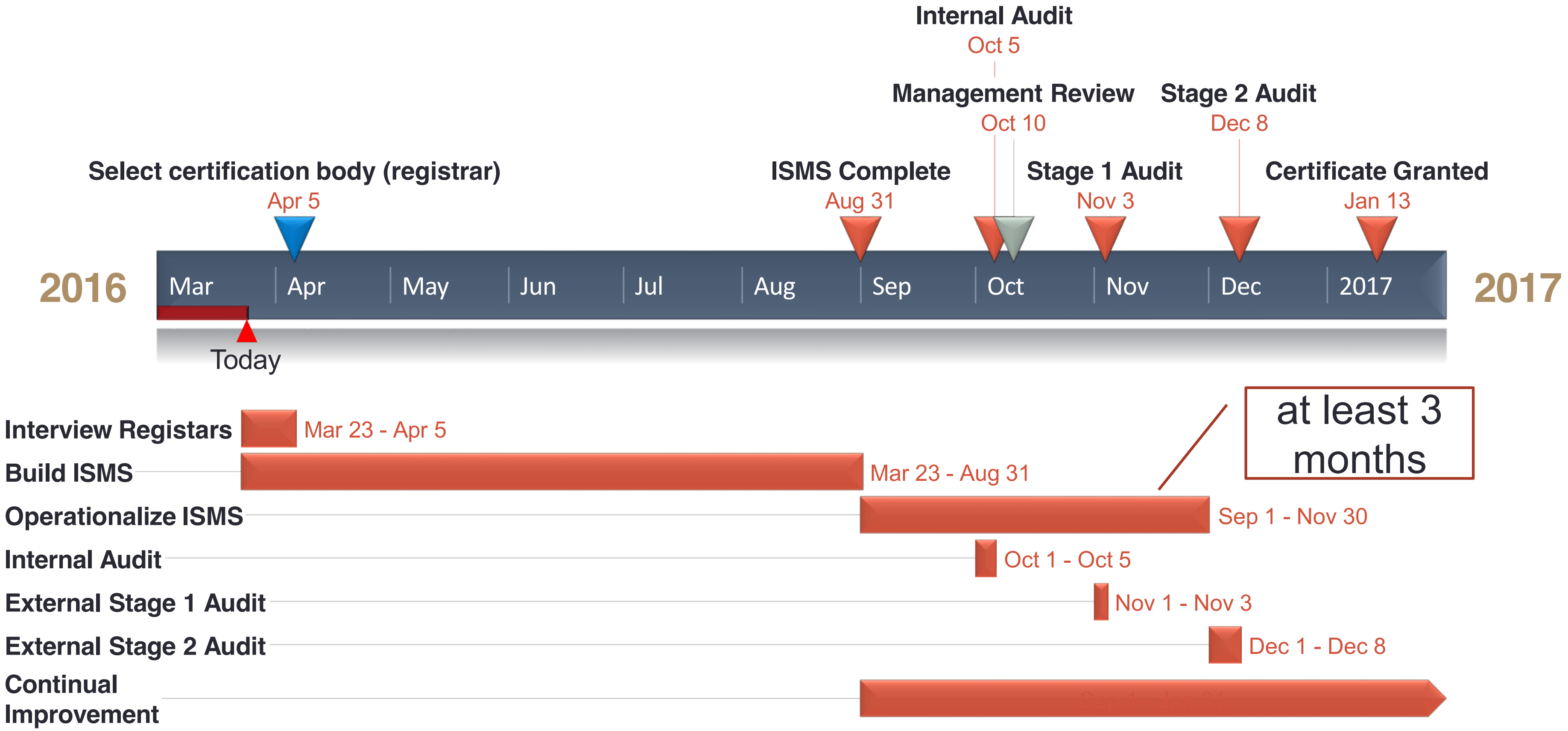
4. Act

- Treatment of Non-conformities
- Continual Improvement

ISO 27001 Advantages

- Improvement of security
- Good governance
- Conformity
- Cost reduction
- Marketing

Certification Timeline

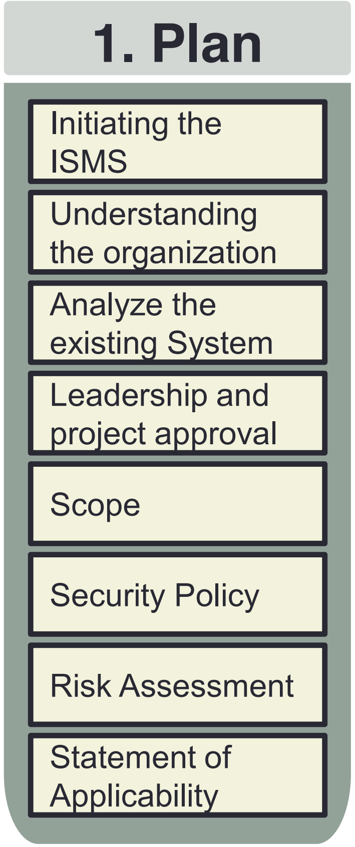


at least 3 months

Surveillance Audits – annually
Recertification Audit – every 3 years

PLANNING THE IMPLEMENTATION

Understanding the Organization

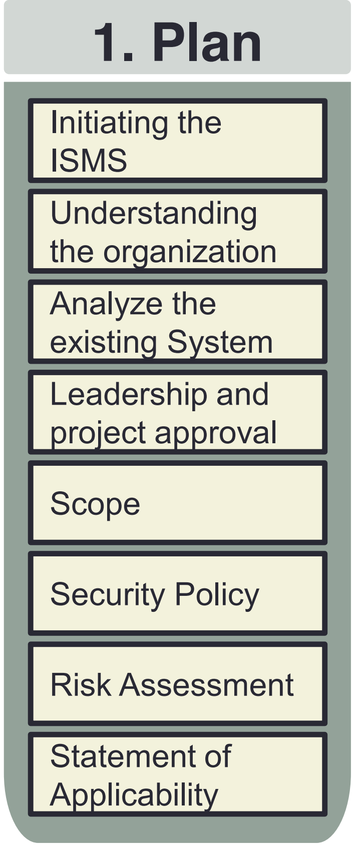


1. Plan

- Initiating the ISMS
- Understanding the organization
- Analyze the existing System
- Leadership and project approval
- Scope
- Security Policy
- Risk Assessment
- Statement of Applicability

- Mission, objectives, values and strategies
- External environment
- Internal environment
- Key processes
- Infrastructure
- Interested parties
- Business Requirements
- ISMS Objectives
- Legal, regulatory and contractual obligations

Analyze the Existing System



1. Plan

Initiating the ISMS

Understanding the organization

Analyze the existing System

Leadership and project approval

Scope

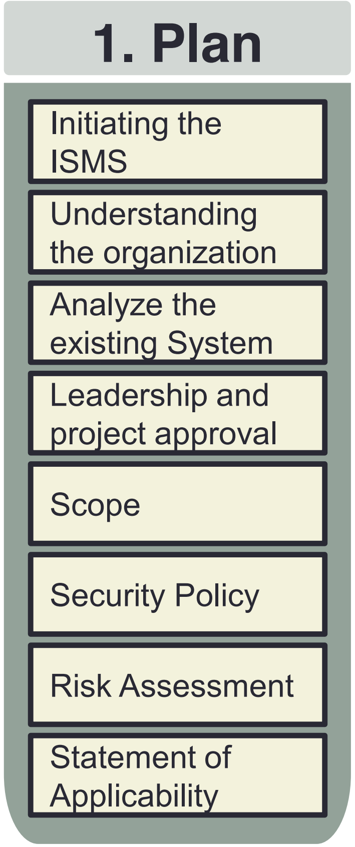
Security Policy

Risk Assessment

Statement of Applicability

- Identify security processes, procedures, plans and measures
- Identify actual level of compliance
- Evaluate effectiveness and maturity level of processes
- Gap analysis (not required by the ISO standard)

Leadership and Project Approval



1. Plan

Initiating the ISMS

Understanding the organization

Analyze the existing System

Leadership and project approval

Scope

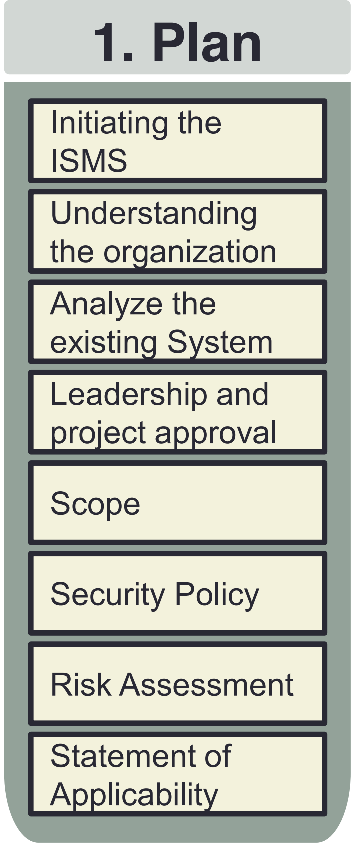
Security Policy

Risk Assessment

Statement of Applicability

- Business case
- Project team
- Steering Committee
- Project plan
- Management approval

Scope

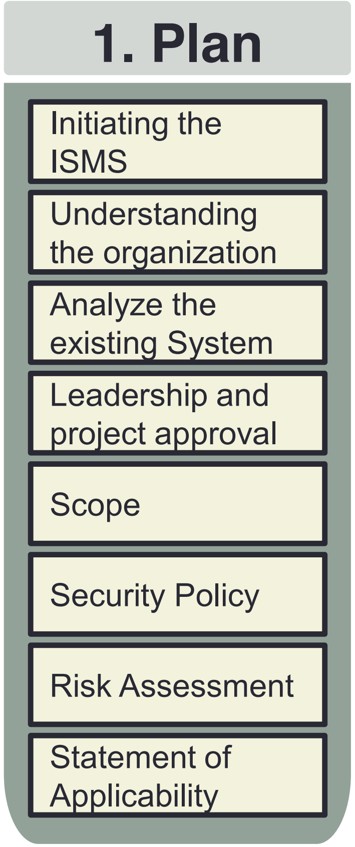


1. Plan

- Initiating the ISMS
- Understanding the organization
- Analyze the existing System
- Leadership and project approval
- Scope
- Security Policy
- Risk Assessment
- Statement of Applicability

- Defines the boundaries (organizational, information system, physical) and applicability of the ISMS
- Helps determine the amount of effort
- Scope can be limited
  - Organizational unit(s)
  - Geographic area
  - Product or Service

Scope



1. Plan

- Initiating the ISMS
- Understanding the organization
- Analyze the existing System
- Leadership and project approval
- Scope
- Security Policy
- Risk Assessment
- Statement of Applicability

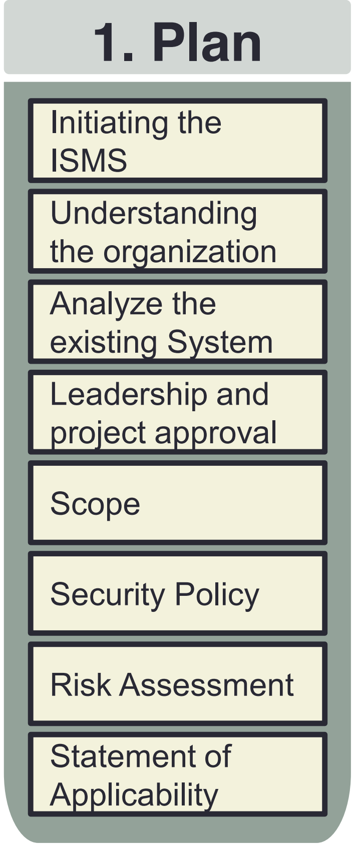
Scope

- Key characteristics of the organization
- Organizational processes
- Descriptions of roles and responsibilities for the ISMS
- List of information assets
- List of information systems
- Details and reasons for exclusions

Scope Statement

- Summary
- Written on the certificate

Security Policy Requirements



1. Plan

Initiating the ISMS

Understanding the organization

Analyze the existing System

Leadership and project approval

Scope

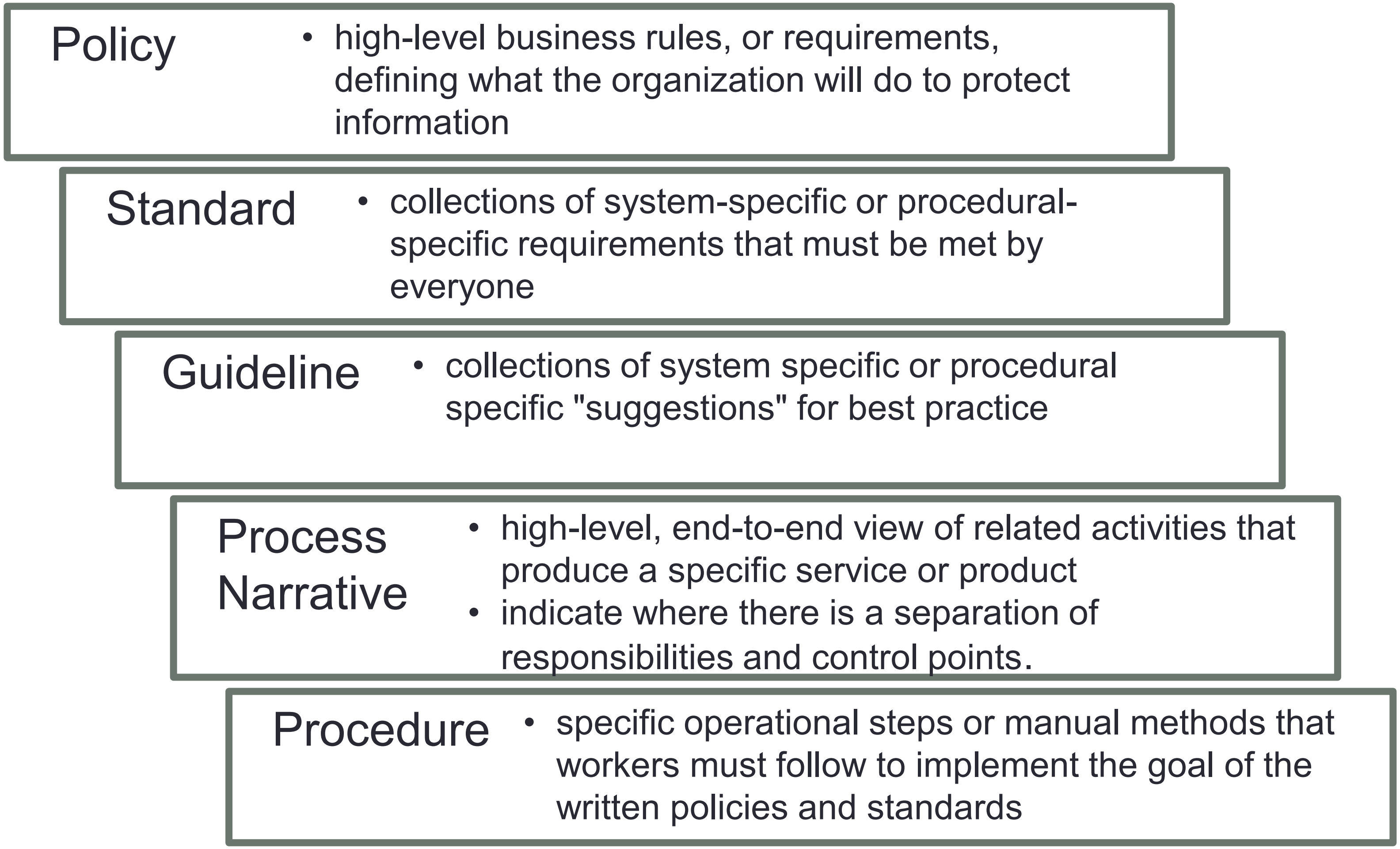
Security Policy

Risk Assessment

Statement of Applicability

- Appropriate to the purpose of the organization
- Commitment to meeting ISO objectives
- Available to the organization as documents
- Communicated within the organization
- Available to interested parties, as appropriate
- ISMS Policy should cover all clauses of ISO 27001
- Security policy can be a single document or separate policy for each ISO 27002 clause
- Can be high level statement of policies with more detail given in subordinate policies

Document Types



Policy
- high-level business rules, or requirements, defining what the organization will do to protect information

Standard
- collections of system-specific or procedural-specific requirements that must be met by everyone

Guideline
- collections of system specific or procedural specific "suggestions" for best practice

Process Narrative
- high-level, end-to-end view of related activities that produce a specific service or product
- indicate where there is a separation of responsibilities and control points.

Procedure
- specific operational steps or manual methods that workers must follow to implement the goal of the written policies and standards

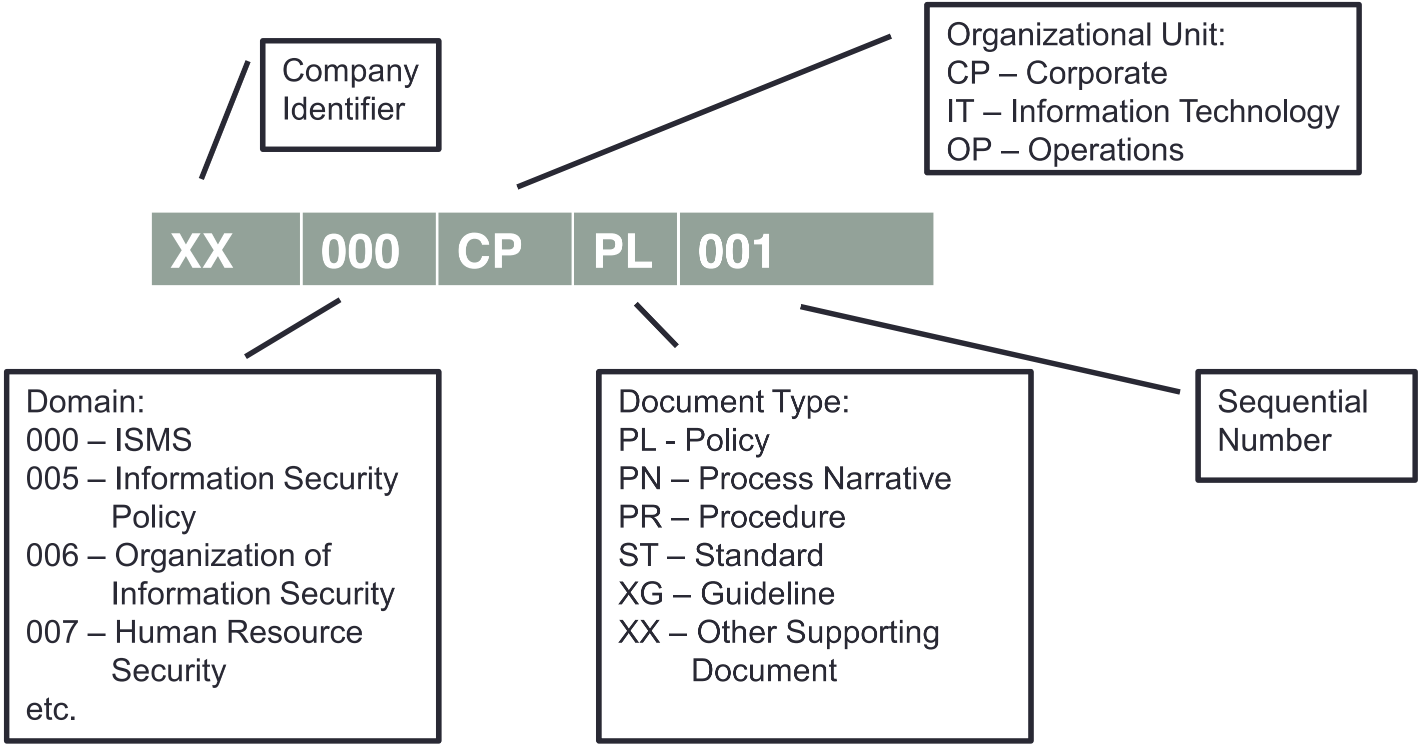
Note: Standards, guidelines and procedures can be included in process narratives or in policies (rare)

Policy Document Structure

- Summary
- Overview
- Scope
- Objectives
- Principles
- Responsibilities
- Enforcement
- Related policies
- Definitions
- Review and approval information
- Version history

Documentation Standard

- Outlines content of each type of document
- Describes the look and identification of the document
- Describes how to review documents
- Defines numbering scheme:



XX	000	CP	PL	001

Company Identifier

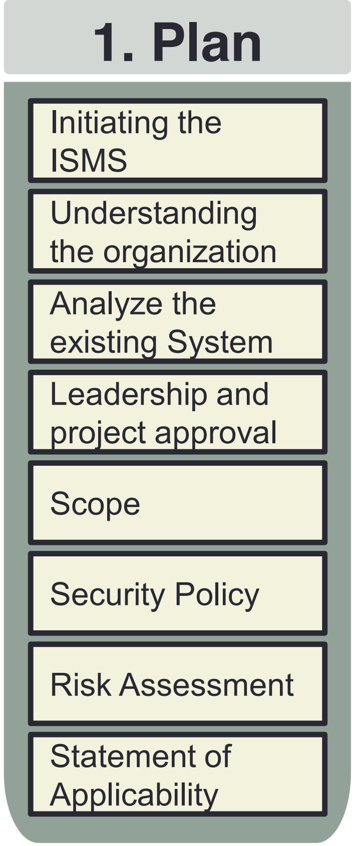
Organizational Unit:
CP – Corporate
IT – Information Technology
OP – Operations

Domain:
000 – ISMS
005 – Information Security Policy
006 – Organization of Information Security
007 – Human Resource Security
etc.

Document Type:
PL - Policy
PN – Process Narrative
PR – Procedure
ST – Standard
XG – Guideline
XX – Other Supporting Document

Sequential Number

Risk Assessment



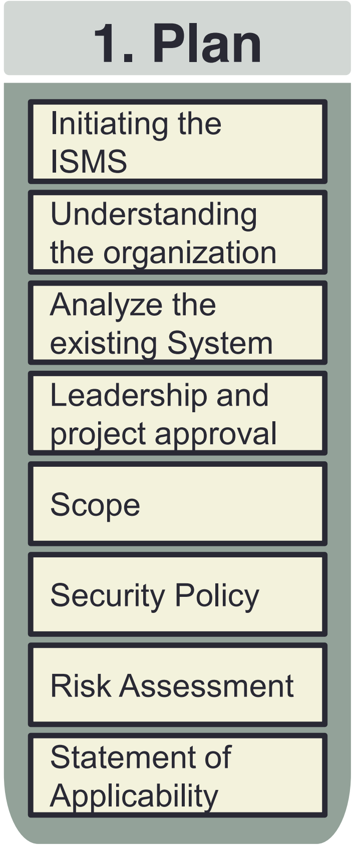
1. Plan

- Initiating the ISMS
- Understanding the organization
- Analyze the existing System
- Leadership and project approval
- Scope
- Security Policy
- Risk Assessment
- Statement of Applicability

- Select risk assessment methodology that will provide comparable and reproducible results
- Determine risks and opportunities that need to be addressed
- Establish and maintain risk criteria
- Select risk treatment options
- Assess control changes, as appropriate
- Formulate risk treatment plan

- ISO 31000 is a generic framework
- ISO 27005 adapts ISO 31000 to information security and is aligned with ISO 27001

Statement of Applicability


1. Plan
Initiating the ISMS
Understanding the organization
Analyze the existing System
Leadership and project approval
Scope
Security Policy
Risk Assessment
Statement of Applicability

A Statement of Applicability shall be produced that includes the following:

1. The necessary control objectives and controls and
2. Justification for inclusions, whether they are implemented or not, and
3. The justification for exclusions of controls from ISO 27001, Annex A

- Must be validated and approved
- One of the first documents that will be analyzed by the certification auditor

DEPLOYING THE ISMS

Organizational Structure

2. Do

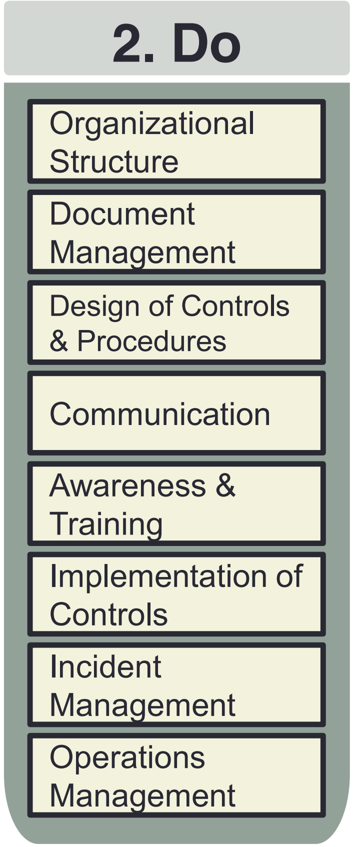
- Organizational Structure
- Document Management
- Design of Controls & Procedures
- Communication
- Awareness & Training
- Implementation of Controls
- Incident Management
- Operations Management

- Governance structure
- Information Security Committee
  - Normally chaired by CISO
- Operational committees, as appropriate

- The Information Security Committee should be described in the ISMS Policy
  - Membership
  - Responsibilities
  - Agenda items for meetings

Document Management

- Documented information required by the standard
- Documented information determined by the organization as being necessary for the effectiveness of the ISMS



- The extent of ISMS documented information can differ by organization
  - Size of the organization
  - Types of activities, processes, products and services
  - Complexity of processes and their interactions,
  - Competence of personnel

Document Management

2. Do

- Organizational Structure
- Document Management
- Design of Controls & Procedures
- Communication
- Awareness & Training
- Implementation of Controls
- Incident Management
- Operations Management

Documents Explicitly Required	Clause
ISMS scope	
Information security policy	5.2
Information security risk assessment process and results	6.1.2 & 8.2
Information security risk treatment process and results	6.1.3 & 8.3
Statement of Applicability	6.1.3d
Information security objectives	6.2
Evidence of competence	7.2d
Control of documented information	7.5
Operational planning and control	8.1
ISMS monitoring and measurement results	9.1
Internal audit programs and audit results	9.2
Management review	9.3
Non-conformities, corrective actions and results	10.1

Design of Controls & Procedures

2. Do

Organizational Structure

Document Management

Design of Controls & Procedures

Communication

Awareness & Training

Implementation of Controls

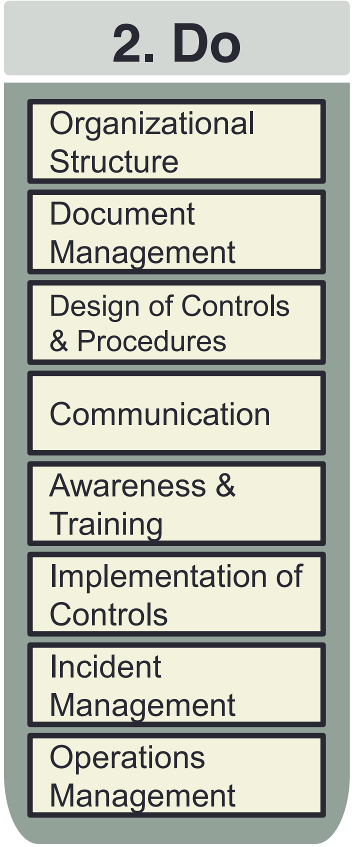
Incident Management

Operations Management

- Controls should be specific and concise
- Should address:
  - Who What When
  - Where Why How
- Example:
  - The network administrator **(Who)** makes sure that backups are completed **(What)** by reviewing backup logs **(How)** each morning **(When)**. Following the review, the network administrator completes and signs a checklist **(Where)** that is retained for future reference **(Why)**.

Note: No requirement to describe in detail each security control, but highly recommended

Communication



2. Do

Organizational Structure

Document Management

Design of Controls & Procedures

Communication

Awareness & Training

Implementation of Controls

Incident Management

Operations Management

- The organization shall determine the need for internal and external communications relevant to the ISMS
  - What to communicate;
  - When to communicate;
  - With whom to communicate;
  - Who shall communicate; and
  - The processes by which communication shall be effected
- Interested parties to consider:
  - Employees
  - Investors
  - Suppliers
  - Customers / Clients
  - Media
  - Communities

Awareness & Training

2. Do

- Organizational Structure
- Document Management
- Design of Controls & Procedures
- Communication
- Awareness & Training
- Implementation of Controls
- Incident Management
- Operations Management

- Ensure the competence of those involved in the operations of the ISMS on the basis of education, training or experience
  - Identify required skills
  - Evaluate education / training needs
  - Implement a training program
- A user who has not been properly informed, trained and made aware of the importance of information security is a potential risk to the security of the organization
- An awareness program is focused on encouraging better security behavior
  - Policy dissemination
  - Information about threats
  - Individual responsibility for security

Implementation of Controls

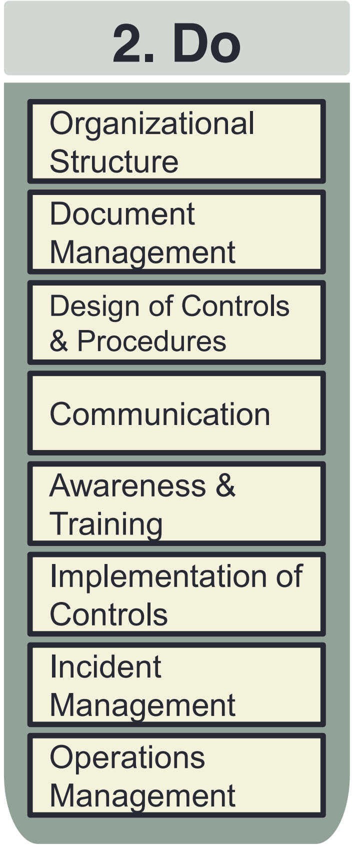
2. Do

- Organizational Structure
- Document Management
- Design of Controls & Procedures
- Communication
- Awareness & Training
- Implementation of Controls
- Incident Management
- Operations Management

Operation Planning and Control

- The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined to address identified risks. The organization shall also implement plans to achieve information security objectives.
- The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.
- The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects.
- The organization shall ensure that outsourced processes are determined and controlled.

Incident Management



2. Do

Organizational Structure

Document Management

Design of Controls & Procedures

Communication

Awareness & Training

Implementation of Controls

Incident Management

Operations Management

- Ensure that security events are detected and identified
- Educate users about the risk factors that could cause security incidents
- Treat security incidents in the most appropriate and effective way
- Reduce the possible impact of incidents on the operations of the organization
- Prevent future security incidents and reduce their change of occurrence
- Improve security controls of the organization by correcting any deficiencies identified following the analysis of security incidents

Note: ISO 27035 is a code of practice for managing information security incidents

Operations Management

2. Do

- Organizational Structure
- Document Management
- Design of Controls & Procedures
- Communication
- Awareness & Training
- Implementation of Controls
- Incident Management
- Operations Management

- Once the ISMS project is complete, the ISMS is transferred to the operations of the organization
- Top management shall demonstrate leadership and commitment with respect to the ISMS by ensuring that the needed resources are available
- The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS

Budget
Tools
Qualified Personnel

MEASUREMENT AND CONTINUAL IMPROVEMENT

Monitoring and Measuring

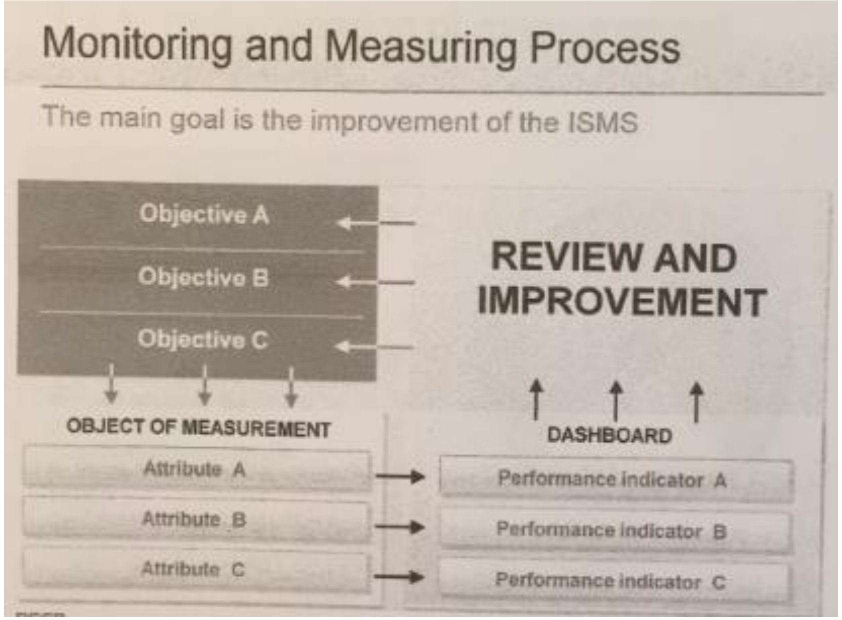
3. Check

Monitoring, Measurement, Analysis and Evaluation

Internal Audit

Management Review

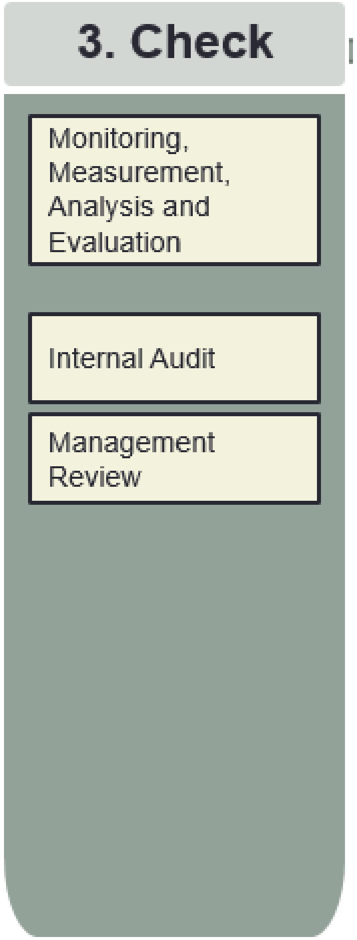
- Identifying the measurement objectives
- Selecting attribute objects that can be measured
- Create performance indicators
- Evaluate if objectives are achieved and improve the management system



Monitoring and Measuring Process

The main goal is the improvement of the ISMS

Internal Audit

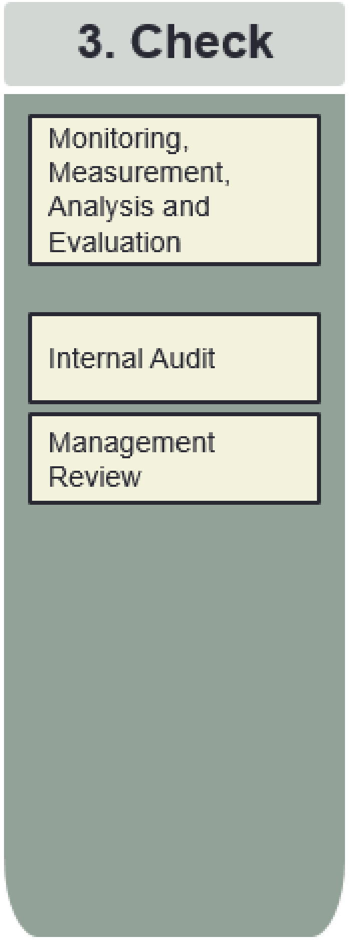


- Types of Audits:
  - First Party Audits (Internal Audit)
  - Second Party Audits (Customer Audit)
  - Third Party Audits (External Independent Audit)
- Audit Charter
- Access and Independence
- Audit Procedures
- Audit Activities

- External / Certification
  - Stage 1
  - Stage 2
  - Surveillance in years 2 and 3

- Non-conformity
  - Major
  - Minor

Management Review



- Performed by top management
- At least annually
- Agenda
  - Status of previous review
  - Changes
  - Non-conformities
  - Monitoring and measuring results
  - Audit results
  - Fulfillment of information security objectives
  - Feedback of interested parties
  - Results of risk assessment / risk treatment
  - Continual improvement opportunities

NEXT STEPS

Assistance / Guidance / Training

- **GRC21**
  - Russ Walsh – russell.walsh@grc21.com 408-582-3645
- **Jim Macellaro Consulting**
  - Jim Macellaro - Jim@jimmacellaro.com 650-269-5141

- **Jim Macellaro** is an IT consultant providing pragmatic technology solutions for business. His primary focus includes: Process Improvement, Information Security Programs, Compliance Assessment (ISO 27701, SOC 2, HIPAA, SOX), Governance and Project Management. Jim has been working with ISO 17799/27001 since 2003. Prior to starting his own firm, Jim held senior leadership positions with Accretive Solutions, GRIC, Ensim, Siemens and IBM. Jim also has numerous certifications, including ISO 27001 Lead Implementer.

- **Russ Walsh** is CEO and Managing Partner of Global Resource Connections (GRC21). The primary focus of GRC21 includes: Information Security (ISO 27001, SOC 1/2/3, HIPAA, SOX, GRC, PCI), CIO Advisory, Internal Audit (Vendor and Supplier Audits, SOX, and Risk/Gap/Vulnerability Assessments. GRC21's team has provided advisory services to many large global companies, including Facebook, Hitachi, Cisco, IBM, EY, Yahoo, Apple, Google, SAP, and Salesforce along with countless startups including, Kaiam, Chirpify, Opsware, and Inflexxion. Prior to starting GRC21, Russ held senior leadership positions with SOAProjects, Opsware, Ernst & Young and Sierra Computing. Russ is also certified in ISO 27001 and instructs students going through the Lead Implementer and Lead Auditor certification process.