ISO 27001 Preparation

Cyber Security Workshop
CBN - SGU -IHP

Kalpin Erlangga Silaen, M.Kom, CISSP, ISO 27001 LI

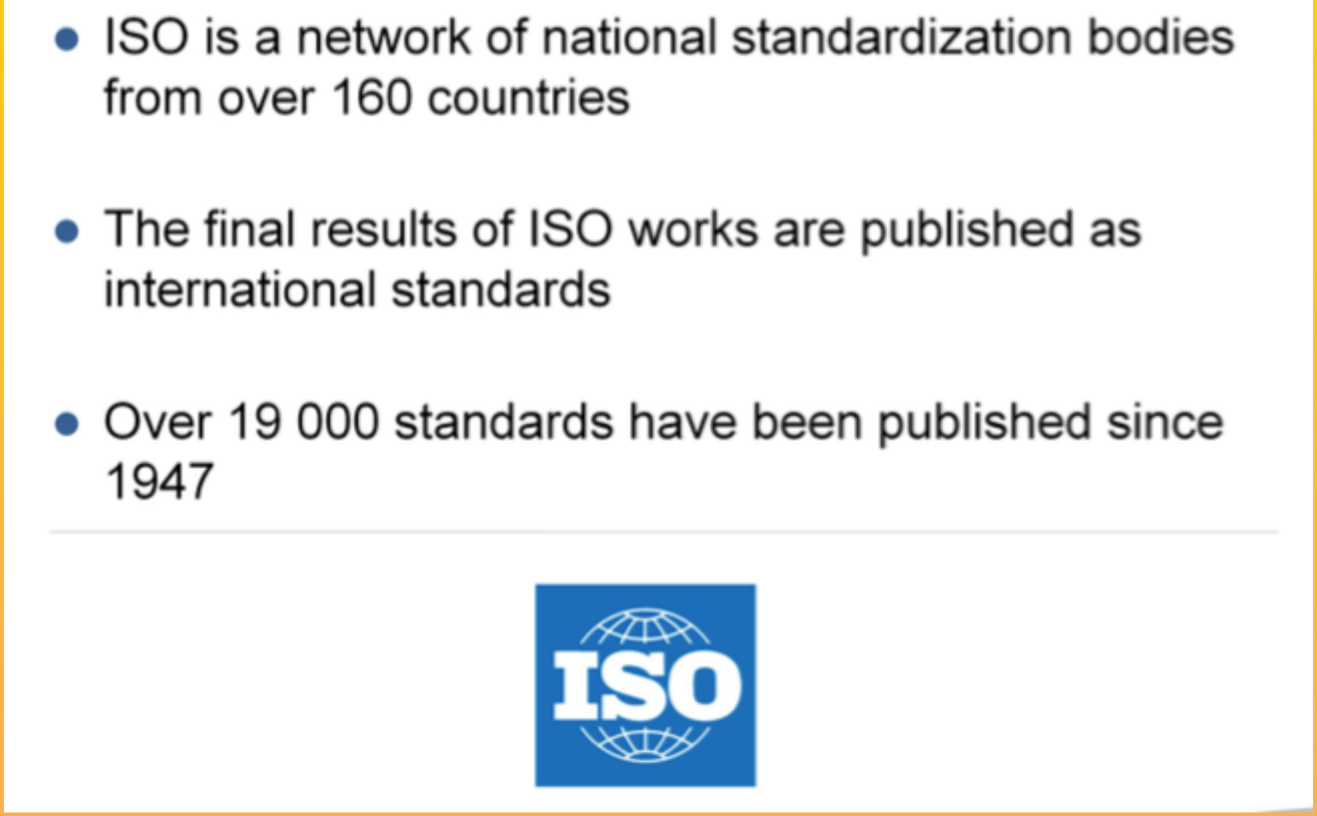
17 May 2017 | Cyber 2 Tower | Jakarta, Indonesia

Indonesia Honeynet Project

CBN

SGU
SWISS GERMAN UNIVERSITY

INTERNATIONAL STANDARD ORGANIZATION (ISO)



- ISO is a network of national standardization bodies from over 160 countries
- The final results of ISO works are published as international standards
- Over 19 000 standards have been published since 1947

ISO 27001 Introduction

- Originally was BS 7799.
- Formally known as "Information technology – Security techniques – Information security management systems – Requirements".
- The formal international security standard and independent certification of information security management system (ISMS).
- ISMS is that part of the overall management system, based on a **business risk approach** to establish, implement, operate, monitor, review, maintain and improve information security

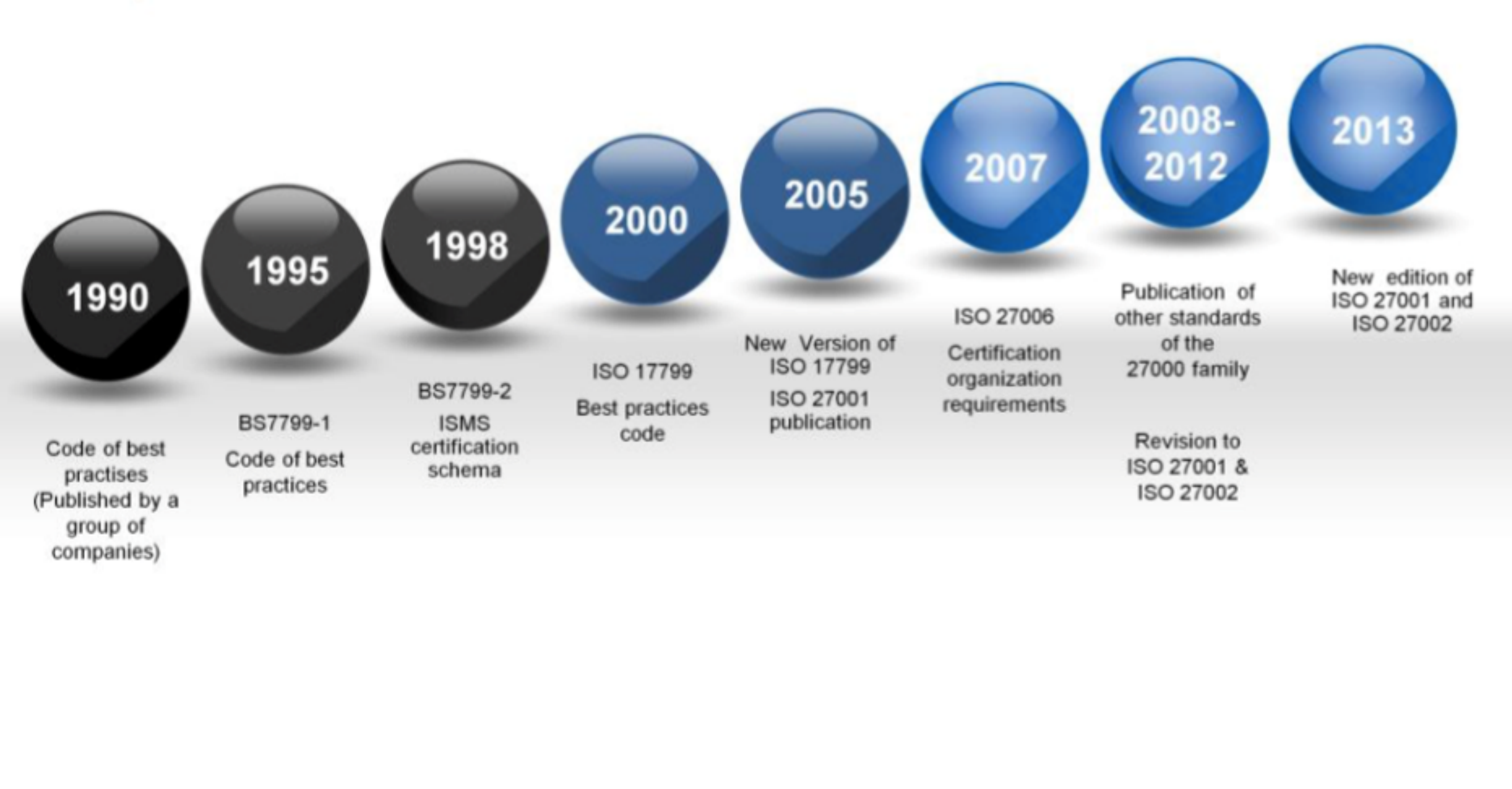
ISO 27001 Introduction (Cont)

- Process Based Approach
- Based on Plan, Do, Check, Act (PDCA) Process Model.
- Stress on **Continual** Process **Improvements.**
- Scope covers **Information Security** not only IT Security.
- Includes People, Process, Technology and Physical.
- Intended to be used in conjunction with ISO 27002 as **guidance on interpretation and implementation** of the ISO 27001 controls.
- 14 security clause headings, 35 security categories, 114 controls

ISO 27001 Introduction (Cont)

- A company or organization must document **its own security goals.**
- All activities must follow a method.
- The method is arbitrary but must be well **defined and documented**.
- The standard offers a set of security controls.
- It is **up to the organization** to choose which controls to implement based on the specific **needs of their business**.
- Security measures used in the ISMS **shall be implemented** as the result of a **documented risk analysis** in order to eliminate or reduce risks to an acceptable level.
- Auditor will verify whether these requirements are fulfilled.

ISO 27001 Development



1990
Code of best practises (Published by a group of companies)

1995
BS7799-1
Code of best practices

1998
BS7799-2
ISMS certification schema

2000
ISO 17799
Best practices code

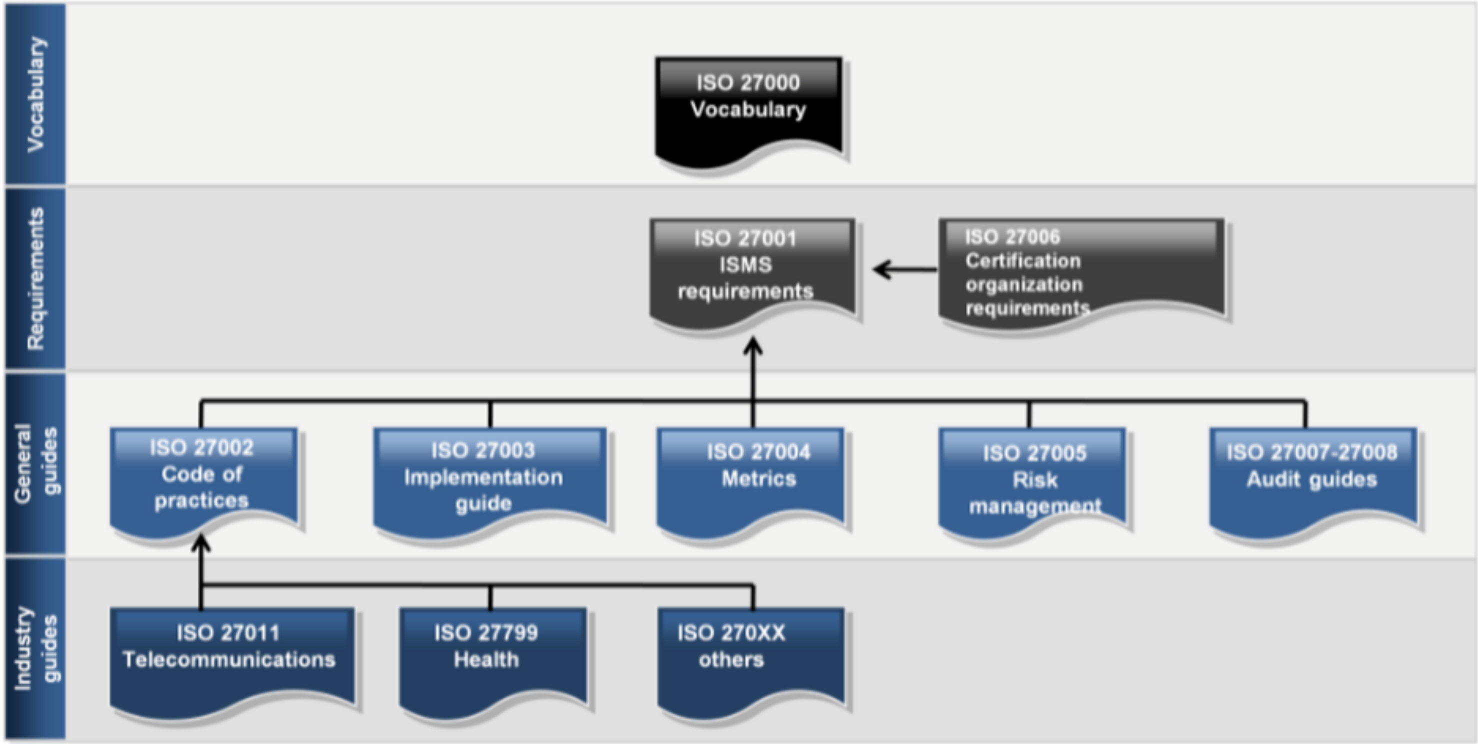
2005
New Version of ISO 17799
ISO 27001 publication

2007
ISO 27006
Certification organization requirements

2008-2012
Publication of other standards of the 27000 family
Revision to ISO 27001 & ISO 27002

2013
New edition of ISO 27001 and ISO 27002

ISO 27000 Series


Vocabulary
Requirements
General guides
Industry guides
ISO 27000 Vocabulary
ISO 27001 ISMS requirements
ISO 27006 Certification organization requirements
ISO 27002 Code of practices
ISO 27003 Implementation guide
ISO 27004 Metrics
ISO 27005 Risk management
ISO 27007-27008 Audit guides
ISO 27011 Telecommunications
ISO 27799 Health
ISO 270XX others

ISO 27001 Relevancy to Organization

- To formulate security requirements and objectives;
- As a way to ensure that security risks are **cost effectively managed**;
- To **ensure compliance** with laws and regulations;
- As a process framework for the implementation and management of controls;
- Definition of new information security management processes;
- To provide relevant information about information security policies, directives, standards and procedures;

ISO 27001 Relevancy to Organization

- Identification and clarification of existing information security management processes;
- Use by the management of organizations to determine the status of information security management activities;
- Use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization;
- Implementation of business-enabling information security;

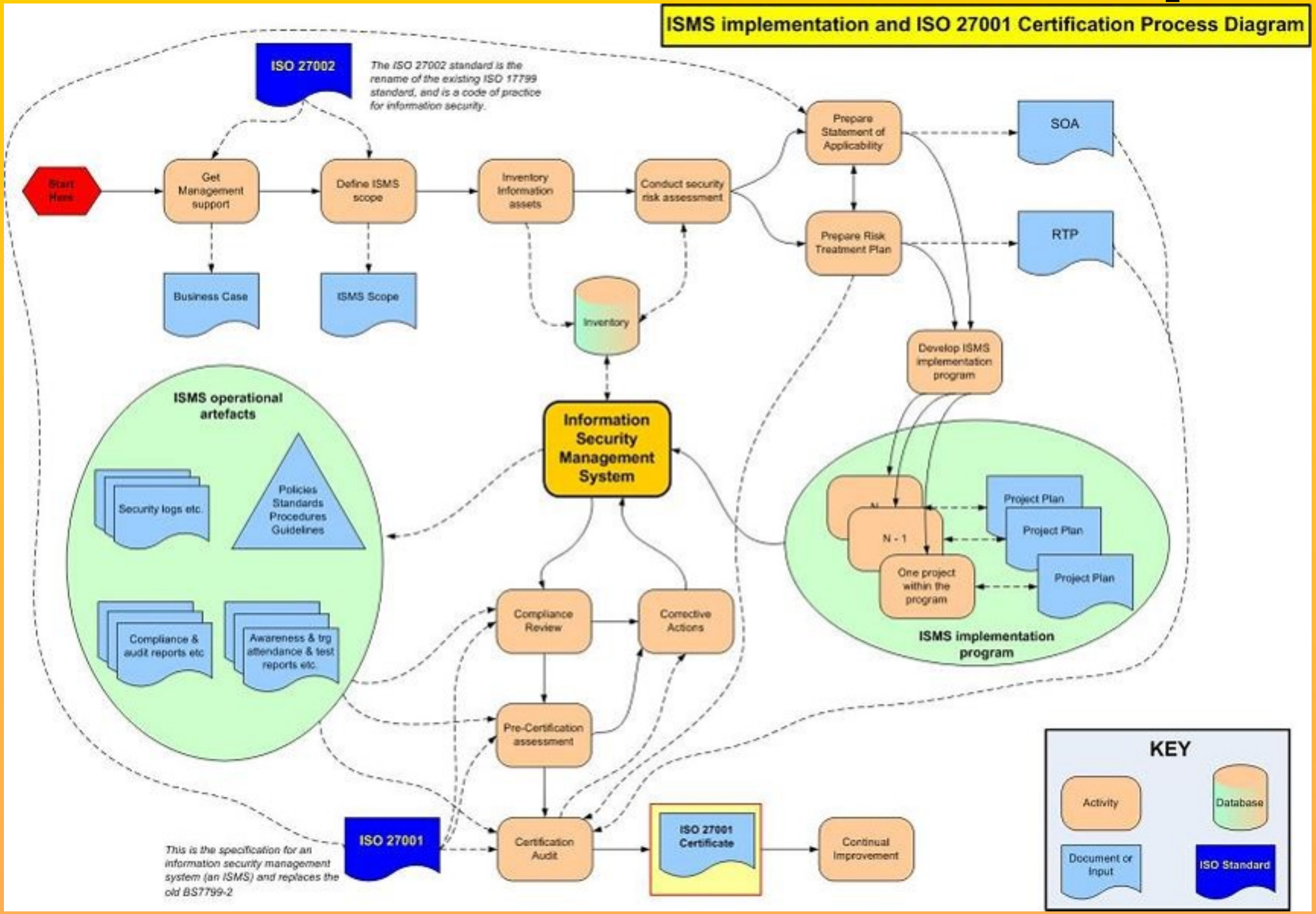
ISMS Benefits

- Improved security for the organization and its clients.
- Increase in the quality of information Security processes and procedures.
- Greater security awareness and ‘buy in’ across all levels of the organization.
- Enhanced customer confidence and perception of the organization.
- Greater awareness of individual roles and responsibilities.

Other Benefits of ISMS

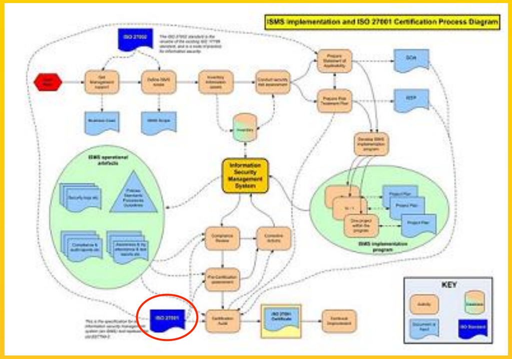
- Increase staff retention
- Protection of brand and reputation
- Reduce costs for correction
- Customer retention
- Tender / competitive advantage
- Instill confidence in clients
- Reduce Financial losses, i.e. insurance, fines and audits
- Reduce security incidents

ISO 27001 - Roadmap


ISMS implementation and ISO 27001 Certification Process Diagram
ISO 27002
The ISO 27002 standard is the rename of the existing ISO 17799 standard, and is a code of practice for information security.
Start Here
Get Management support
Define ISMS scope
Inventory Information assets
Conduct security risk assessment
Prepare Statement of Applicability
SOA
Prepare Risk Treatment Plan
RTP
Business Case
ISMS Scope
Inventory
Develop ISMS implementation program
ISMS operational artefacts
Security logs etc.
Policies Standards Procedures Guidelines
Compliance & audit reports etc
Awareness & trg attendance & test reports etc.
Information Security Management System
N
N - 1
One project within the program
Project Plan
Project Plan
Project Plan
ISMS implementation program
Compliance Review
Corrective Actions
Pre-Certification assessment
Certification Audit
ISO 27001 Certificate
Continual Improvement
ISO 27001
This is the specification for an information security management system (an ISMS) and replaces the old BS7799-2
KEY
Activity
Database
Document or Input
ISO Standard

References:
ISO 27001
Security

ISO 27001

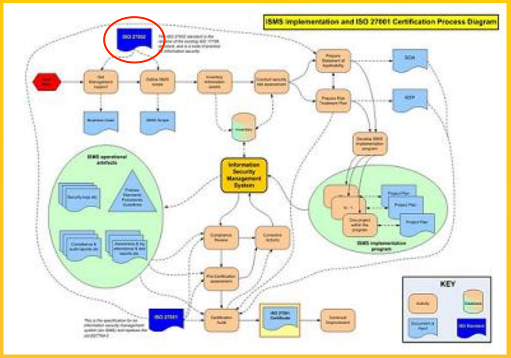

ISMS implementation and ISO 27001 Certification Process Diagram
ISO 27002
SOA
RTP
ISMS operational artifacts
Information Security Management System
ISMS implementation program
Project Plan
Project Plan
Project Plan
ISO 27001
ISO 27001 Certificate
KEY

ISO27001

- ISO27001 formally specifies how to establish an Information Security Management System (ISMS).
- The adoption of an ISMS is a strategic decision.
- The design and implementation of an organization’s ISMS is influenced by its business and security objectives, its security risks and control requirements, the processes employed and the size and structure of the organization: a simple situation requires a simple ISMS.
- The ISMS will evolve systematically in response to changing risks.
- Compliance with ISO27001 can be formally assessed and certified. A certified ISMS builds confidence in the organization’s approach to information security management among stakeholders.

www.ISO27001security.com

ISO 27002

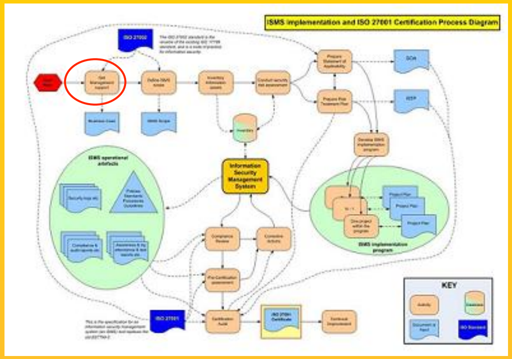

ISMS implementation and ISO 27001 Certification Process Diagram
KEY

ISO27002

- ISO27002 is a “Code of Practice” recommending a large number of information security controls.
- Control objectives throughout the standard are generic, high-level statements of business requirements for securing or protecting information assets.
- The numerous information security controls recommended by the standard are meant to be implemented in the context of an ISMS, in order to address risks and satisfy applicable control objectives systematically.
- Compliance with ISO27002 implies that the organization has adopted a comprehensive, good practice approach to securing information.

www.ISO27001security.com

Management Support

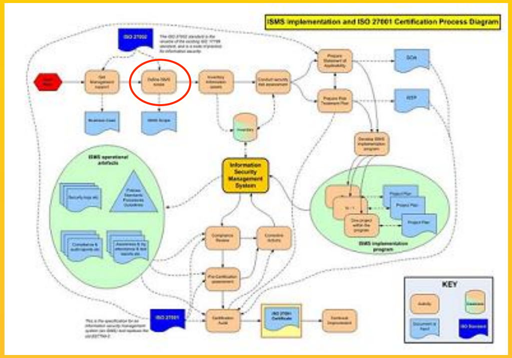

ISMS implementation and ISO 27001 Certification Process Diagram
ISO 27002
Get Management support
Define ISMS scope
Inventory information assets
Conduct security risk assessment
Prepare Statement of Applicability
Prepare Risk Treatment Plan
SOA
RTP
Business Case
ISMS Scope
Inventory
Develop ISMS implementation program
Information Security Management System
ISMS operational artifacts
Security logs etc.
Policies Standards Procedures Guidelines
Compliance & audit reports etc.
Awareness & trg attendance & test results etc.
Project Plan
One project within the program
ISMS implementation program
Compliance Review
Corrective Actions
Pre-Certification assessment
Certification Audit
ISO 27001
ISO 27001 Certificate
Continual Improvement
KEY
Activity
Document or Input
ISO Standard

Management support is vital

- Management should actively support information security by giving clear direction (*e.g.* policies), demonstrating the organization's commitment, plus explicitly assigning information security responsibilities to suitable people.
- Management should approve the information security policy, allocate resources, assign security roles and co-ordinate and review the implementation of security across the organization.
- Overt management support makes information security more effective throughout the organization, not least by aligning it with business and strategic objectives.

www.ISO27001security.com

Defining ISMS Scope

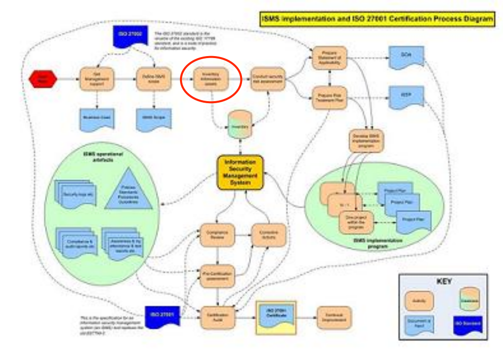


Define ISMS scope

- Management should define the scope of the ISMS in terms of the nature of the business, the organization, its location, information assets and technologies.
- Any exclusions from the ISMS scope should be justified and documented.
  - Areas outside the ISMS are inherently less trustworthy, hence additional security controls may be needed for any business processes passing information across the boundary.
  - De-scoping usually reduces the business benefits of the ISMS.
- If commonplace controls are deemed not applicable, this should be justified and documented in the Statement of Applicability (SOA)
- The certification auditors will check the documentation.

www.ISO27001security.com

Inventory of Assets

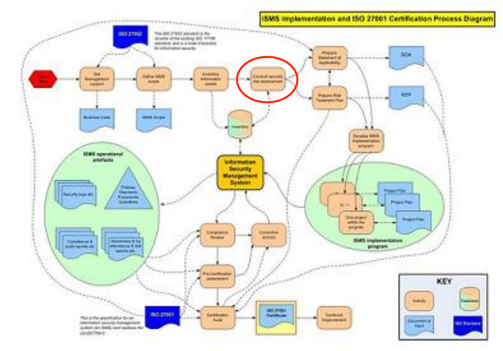

ISMS implementation and ISO 27001 Certification Process Diagram
ISO 27002
Get Management support
Define ISMS scope
Inventory information assets
Conduct security risk assessment
Prepare Statement of Applicability
Prepare Risk Treatment Plan
SOA
RTP
Business Case
ISMS Scope
Inventory
Develop ISMS implementation program
Information Security Management System
ISMS operational artifacts
Policies Standards Procedures Guidelines
Project Plan
ISMS implementation program
Compliance Review
Corrective Actions
Pre-Certification assessment
Certification Audit
ISO 27001
ISO 27001 Certificate
Continual Improvement
KEY
Activity
Database
Document & Report
ISO Standard

Inventory information assets

- An inventory of all important information assets should be developed and maintained, recording details such as:
  - Type of asset;
  - Format (*i.e.* software, physical/printed, services, people, intangibles)
  - Location;
  - Backup information;
  - License information;
  - Business value (*e.g.* what business processes depend on it?).

www.ISO27001security.com

Risk Assessment

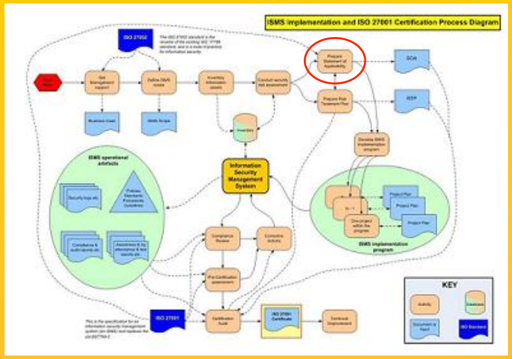

ISMS implementation and ISO 27001 Certification Process Diagram
ISO 27002
Conduct security risk assessment
Prepare Statement of Applicability
Prepare Risk Treatment Plan
SOA
RTP
Business Case
ISMS Scope
Inventory
Information Security Management System
ISMS operational artefacts
ISMS implementation program
Project Plan
Compliance Review
Corrective Actions
Pre-Certification assessment
Certification Audit
ISO 27001
ISO 27001 Certificate
Continual Improvement
KEY

Assess information security risks

- Risk assessments should identify, quantify, and prioritize information security risks against defined criteria for risk acceptance and objectives relevant to the organization.
- The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.
- Assessing risks and selecting controls may need to be performed repeatedly across different parts of the organization and information systems, and to respond to changes.
- The process should systematically estimate the magnitude of risks (risk analysis) and compare risks against risk criteria to determine their significance (risk evaluation).
- The information security risk assessment should have a clearly defined scope and complement risk assessments in other aspects of the business, where appropriate.

www.ISO27001security.com

Prepare Statement of Applicability

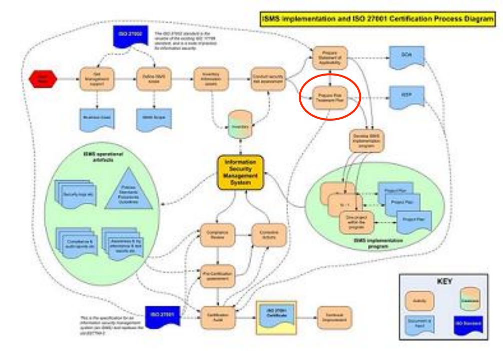

ISMS Implementation and ISO 27001 Certification Process Diagram
ISO 27002
Prepare Statement of Applicability
SOA
Prepare Risk Treatment Plan
RTP
Business Case
ISMS Scope
Inventory
Information Security Management System
ISMS operational artifacts
Develop ISMS implementation program
Project Plan
Project Plan
Project Plan
ISMS implementation program
Compliance Review
Corrective Actions
Pre-Certification assessment
Certification Audit
ISO 27001
ISO 27001 Certificate
Continual Improvement
KEY
Activity
Database
Document & Report
ISO Standard

SOA

- The Statement of Applicability (SOA) is a key ISMS document listing the organization's information security control objectives and controls.
- The SOA is derived from the results of the risk assessment, where:
  - Risk treatments have been selected;
  - All relevant legal and regulatory requirements have been identified;
  - Contractual obligations are fully understood;
  - A review the organization's own business needs and requirements has been carried out.

www.ISO27001security.com

Prepare Risk Treatment Plan

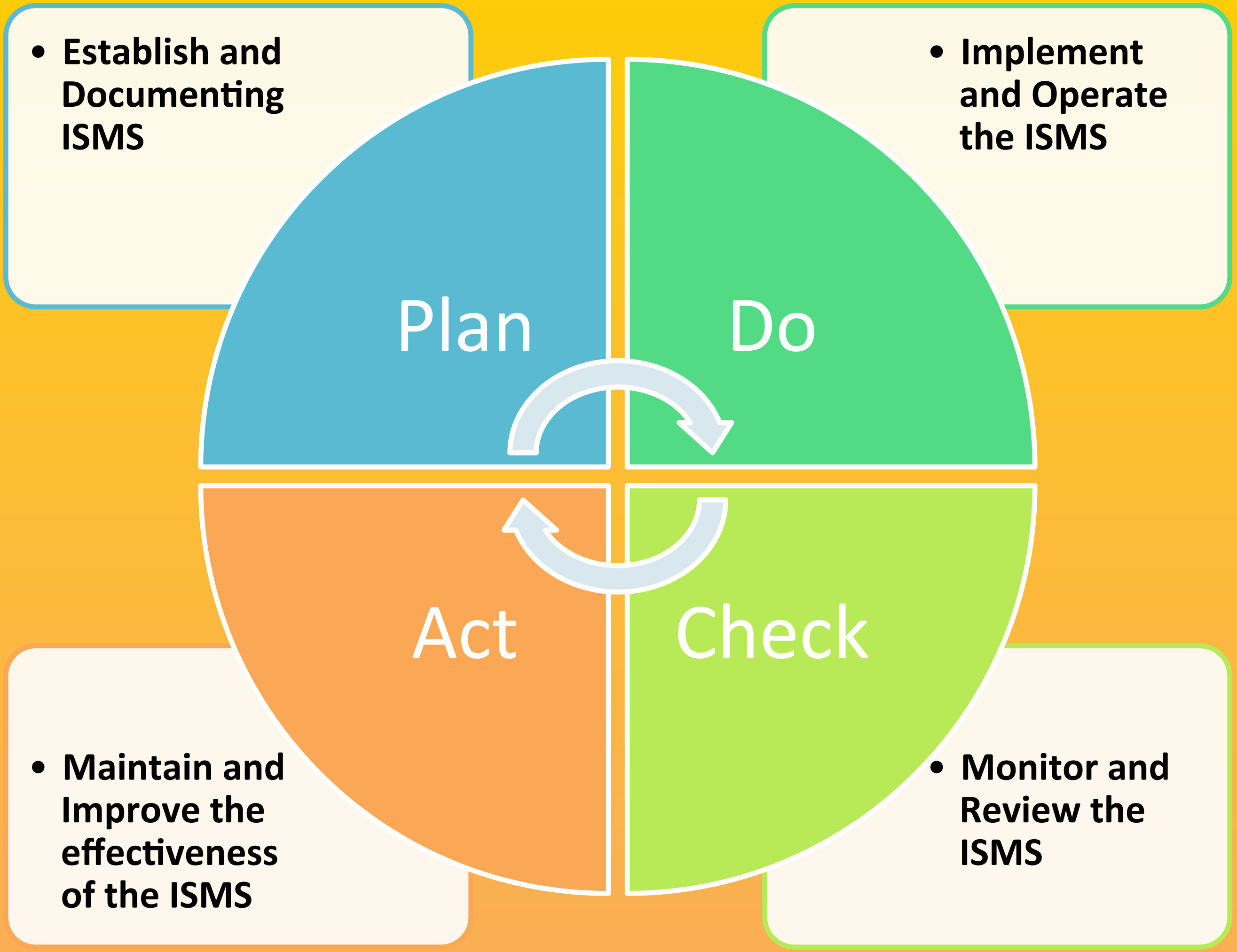

ISMS implementation and ISO 27001 Certification Process Diagram
ISO 27002
SOA
RTP
Information Security Management System
ISMS operational artefacts
ISMS implementation program
Project Plan
Project Plan
Project Plan
ISO 27001
ISO 27001 Certificate
KEY

Prepare Risk Treatment Plan

- The organisation should formulate a risk treatment plan (RTP) identifying the appropriate management actions, resources, responsibilities and priorities for dealing with its information security risks.
- The RTP should be set within the context of the organization's information security policy and should clearly identify the approach to risk and the criteria for accepting risk.
- The RTP is the key document that links all four phases of the PDCA cycle for the ISMS (next 2 slides).

www.ISO27001security.com

PDCA Model



- Establish and Documenting ISMS

- Implement and Operate the ISMS

Plan

Do

Act

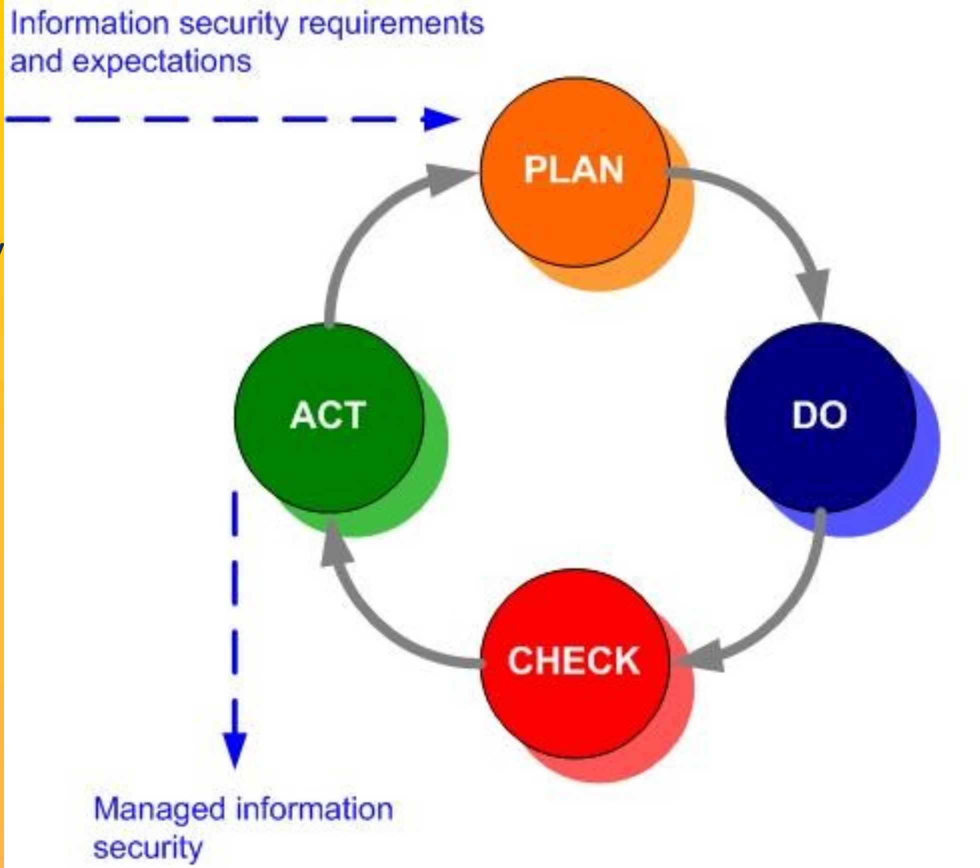
Check

- Maintain and Improve the effectiveness of the ISMS

- Monitor and Review the ISMS

PDCA Model

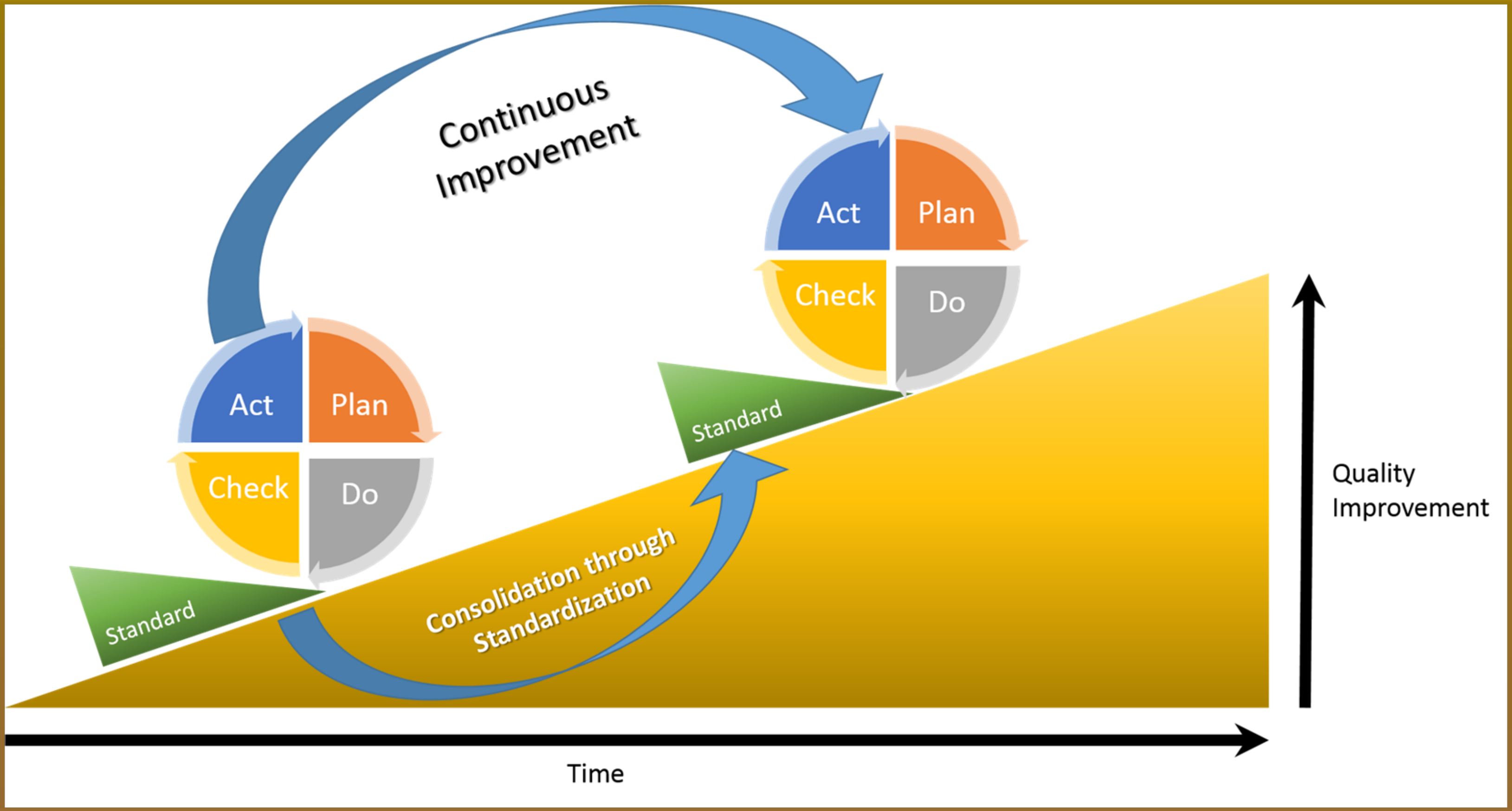
- The "Plan-Do-Check-Act" (PDCA) model applies at different levels throughout the ISMS (cycles within cycles).
- The same approach is used for quality management in ISO9000.
- The diagram illustrates how an ISMS takes as input the information security requirements and expectations and through the PDCA cycle produces managed information security outcomes that satisfy those requirements and expectations.



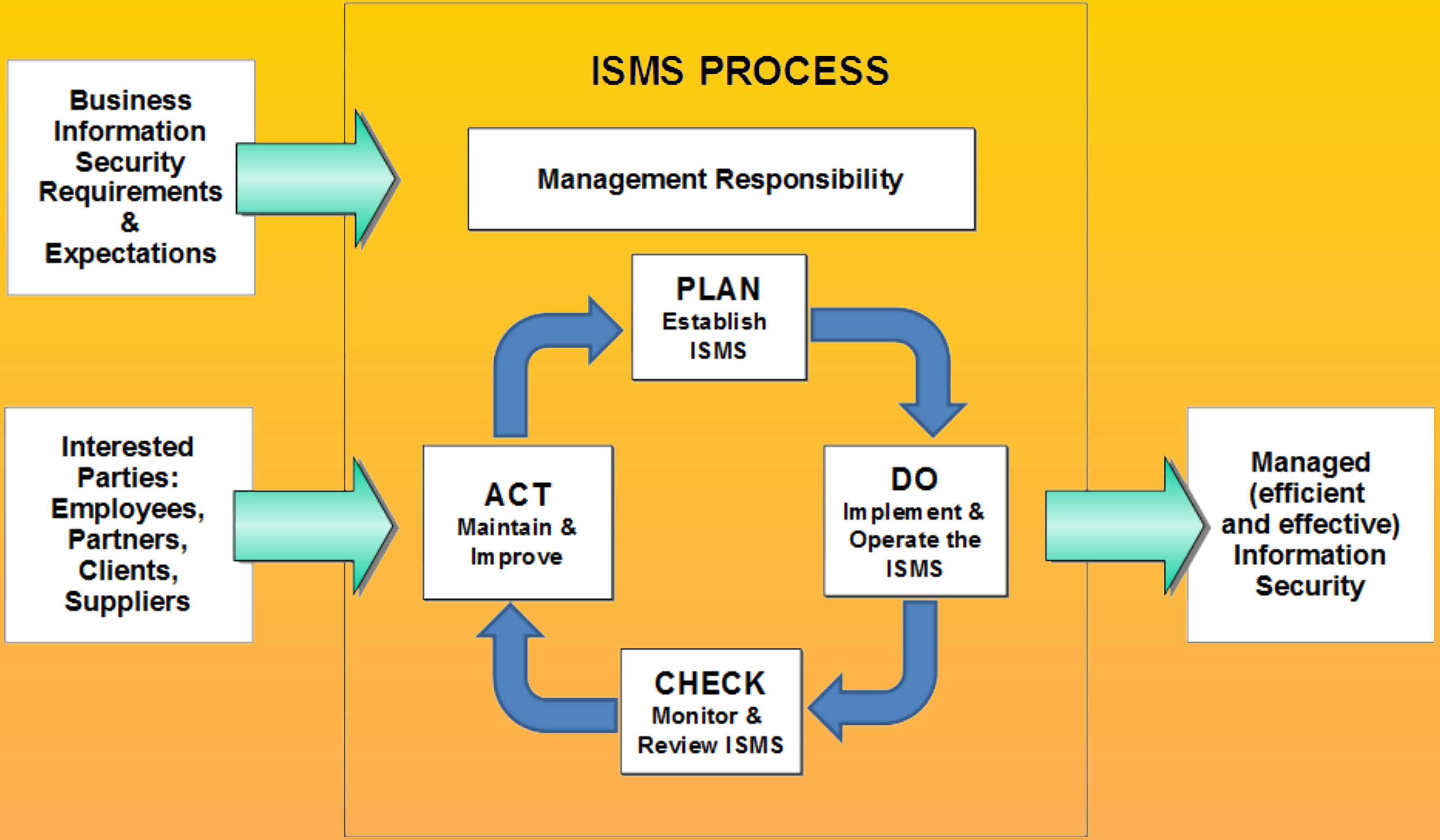
Information security requirements and expectations
PLAN
DO
CHECK
ACT
Managed information security

www.ISO27001security.com

PDCA Model (Cont)



ISMS Process and PDCA Model



Business Information Security Requirements & Expectations

Interested Parties: Employees, Partners, Clients, Suppliers

ISMS PROCESS

Management Responsibility

PLAN
Establish ISMS

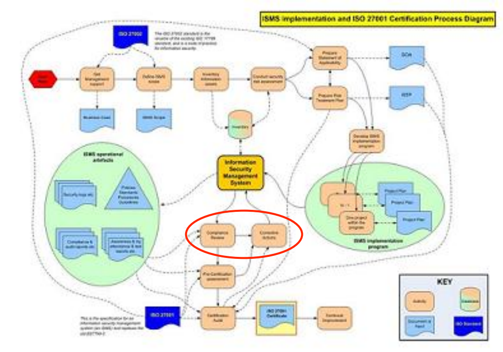
DO
Implement & Operate the ISMS

CHECK
Monitor & Review ISMS

ACT
Maintain & Improve

Managed (efficient and effective) Information Security

Compliance Review and Corrective Actions


ISMS implementation and ISO 27001 Certification Process Diagram
ISO 27002
ISO 27001
KEY

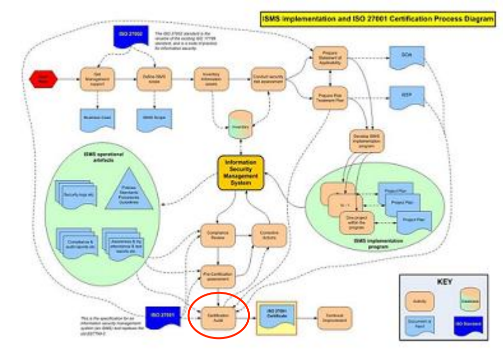
Compliance Review

Corrective actions

- Management must review the organization’s ISMS at least once a year to ensure its continuing suitability, adequacy and effectiveness.
- They must assess opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives.
- The results of these reviews must be clearly documented and maintained (“records”).
- Reviews are part of the ‘Check’ phase of the PDCA cycle: any corrective actions arising must be managed accordingly.

www.ISO27001security.com

Certification Audit

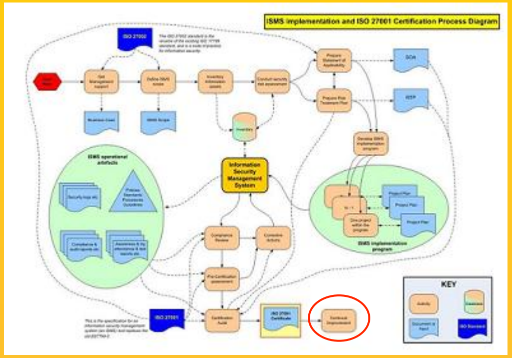

ISMS implementation and ISO 27001 Certification Process Diagram
ISO 27002
SOA
RTP
Inventory
ISMS operational artefacts
Information Security Management System
ISMS implementation program
ISO 27001
KEY

Certification Audit

- Certification involves the organization’s ISMS being assessed for compliance with ISO27001.
- The certification body needs to gain assurance that the organization’s information security risk assessment properly reflects its business activities for the full scope of the ISMS.
- The assessors will check that the organization has properly analysed and treated its information security risks and continues managing its information security risks systematically.
- A certificate of compliance from an accredited certification body has credibility with other organizations

www.ISO27001security.com

Certification Audit (Cont)


ISMS implementation and ISO 27001 Certification Process Diagram
ISO 27002
SOA
RTP
ISMS operational artifacts
Information Security Management System
ISMS implementation program
Project Plan
Project Plan
Project Plan
ISO 27001
ISO 27001 Certificate
KEY

Continual Improvement

- The organization shall continually improve the effectiveness of the ISMS through the use of:
  - The information security policy;
  - Information security objectives;
  - Audit results;
  - Analysis of monitored events;
  - Corrective and preventive actions;
  - Management review.

www.ISO27001security.com

Backspace
Scree
Page Up
Home
Thank You
Page Down
"
'
Shift
Insert