ISO/IEC 27000:2009

ISO/IEC 27000:2009

A new standard for "information security management"

Marc Vael

SAI
studiecentrum voor automatische informatieverwerking vzw

Information Security Threats

- Imposition of legal & regulatory obligations.
- Cyber-criminals
- Malware, Trojans
- Phishers
- Spammers
- Negligent staff
- Acts of God
- Hackers
- Unethical employees misusing/misconfiguring system security functions
- Unauthorized access, modification, disclosure of information assets
- Nations attacking critical information infrastructures to cause disruption.
- Technical advances that can render encryption algorithms obsolete

SAI

(Survey 2008 ISO27X FORUM)

ACROSS TECHNOLOGY

ISO/IEC 27000:2009

Information Security Impacts

Resulting information security incidents can cause:

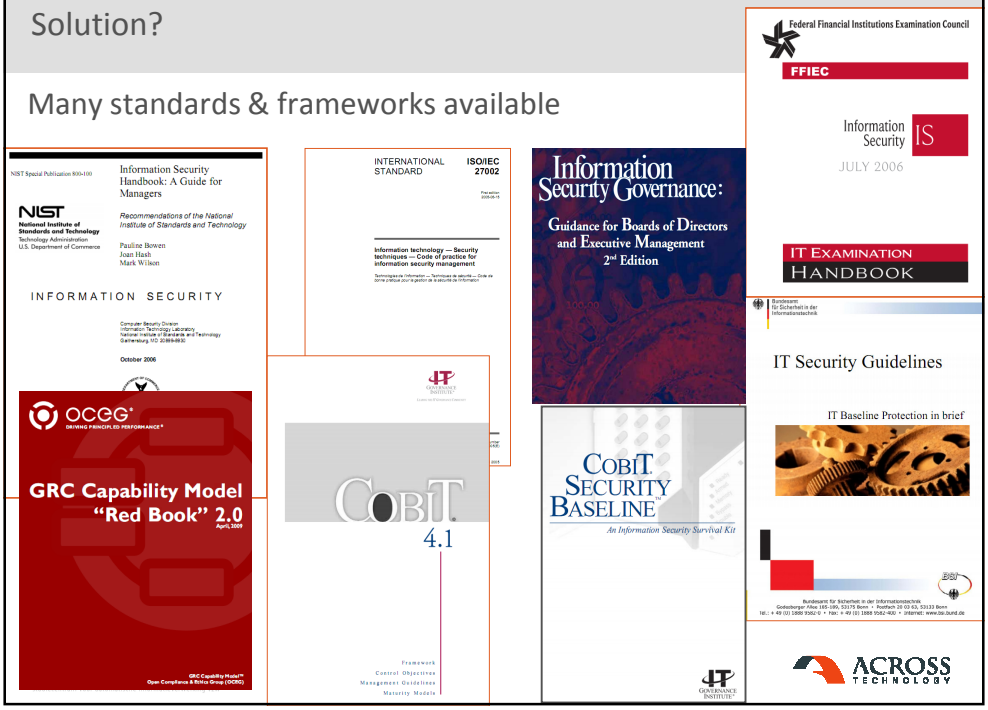
- Disruption to organizational routines and processes
- Direct financial losses through information theft & fraud
- Decrease in shareholder value
- Loss of privacy
- Reputational damage causing brand devaluation
- Loss of confidence in IT
- Expenditure on information security assets & data damaged, stolen, corrupted or lost in incidents
- Loss of competitive advantage
- Reduced profitability
- Impaired growth due to inflexible infrastructure/system/application environments
- Injury or loss of life if safety-critical systems fail

SAI studiecentrum voor automatische informatieverwerking vzw

ACROSS TECHNOLOGY

Solution?

Many standards & frameworks available



ISO/IEC 27000:2009

Solution?

SAI

ACROSS TECHNOLOGY

Solution?

Computer Dictionary — Activate your FREE membership today | Log-in

Whatis?com
The leading IT encyclopedia and learning center

HOME · SEARCH · BROWSE BY CATEGORY · BROWSE BY ALPHABET · FILE EXTENSION LIST · CHEAT SHEETS · WHITE PAPERS

LOOK IT UP Definitions for thousands of the most current IT-related words.
Search our IT-specific encyclopedia for: Search

Browse alphabetically:
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z #

Browse for technology definitions by category:

- Computing fundamentals
- Data and data management
- Hardware
- Network management
- Programming
- Security
- Internet technology and lingo
- Browse all tech definition categories

Word of the Day

Mobile device management (MDM) refers to any routine or tool intended to distribute applications, data and configuration settings to mobile communications devices, such as laptop computers, cell phones and PDAs. The intent of MDM is to optimize the functionality and security of a mobile communications network, while minimizing cost and downtime.

Overheard talking about the Word of the Day

Are you a Know-IT-All?
Spock had an ___ ____ in the Star Trek mirror universe -- in a WLAN context, it describes a counterfeit access point.
Answer

Get the Word of the Day
Follow us on Twitter

What's New

WORD OF THE DAY...
mobile device management

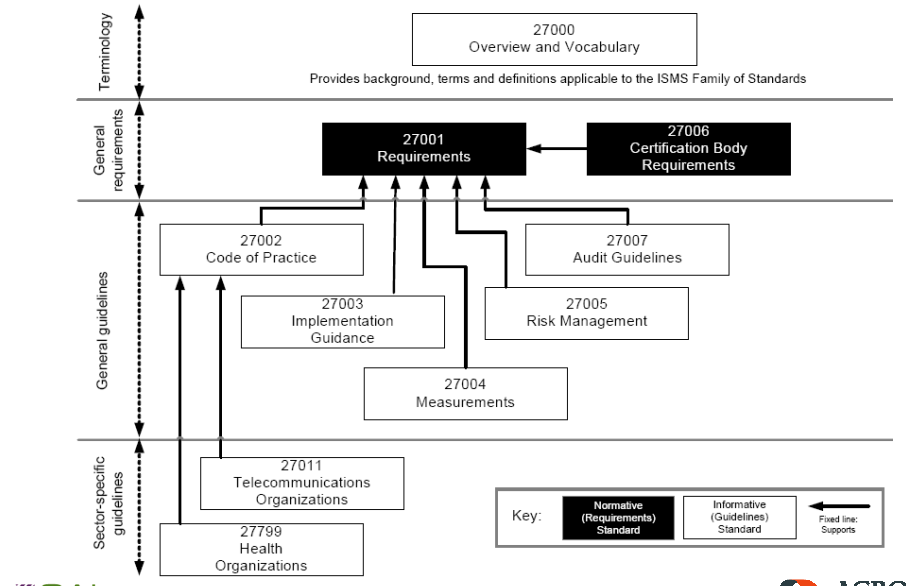
LEARN MORE ABOUT...
CRM

- USA Contributors
- Worldwide Contributors
- Awards and Recognition
- Our 60+ tech-specific sites

WhatIs.com RSS Feeds

ISO/IEC 27000:2009

ISO/IEC 27000:2009 Overview



SAI

ACROSS TECHNOLOGY

ISO 27001 ISMS Requirements

ISMS Certification

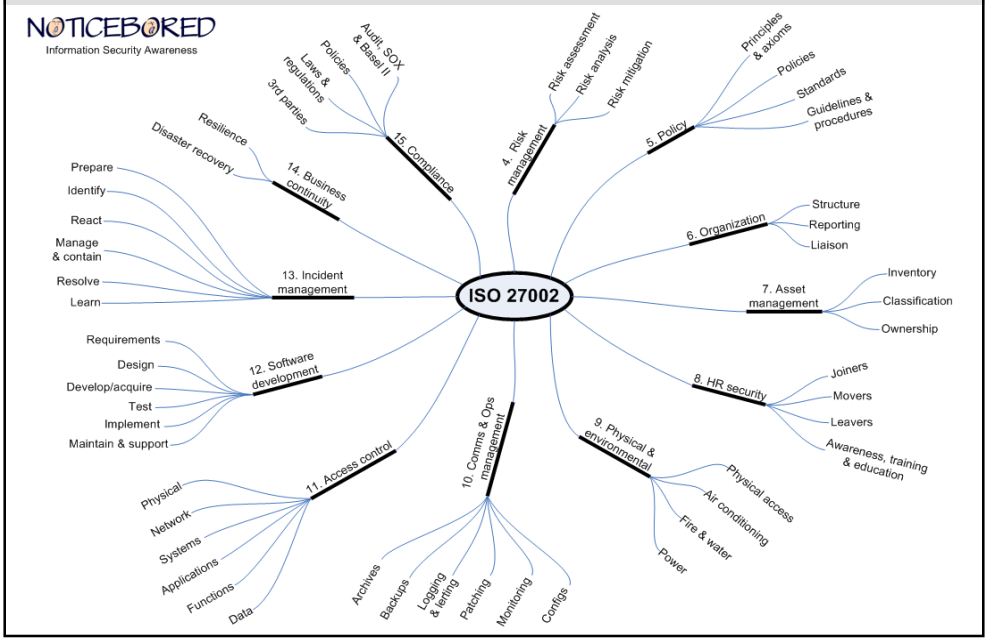
- Composed of
  - core document : process of certification
  - annex A : mandatory controls 17799
- ISO 27001 : “comprehensive” compulsory reference
- Proportionality principle persist but must be justified
- Statement Of Applicability (SOA)
  - relevant to the organization
  - shall include
    - all control objectives of annex A
    - controls currently implemented
    - exclusions with justification

SAI

ACROSS TECHNOLOGY

ISO/IEC 27000:2009

ISO 27001 ISMS Code of Practice



ISO 27003 ISMS Implementation Guidelines

- Scope: practical implementation guidance & further information for establishing, implementing, operating, monitoring, reviewing, maintaining and improving ISMS in accordance with ISO/IEC 27001.
  - Detailed advice & help regarding PDCA processes
  - ISMS Scope & Policy
  - Identification of assets
  - Monitoring & review
  - Continuous Improvement
- Purpose: ISO/IEC 27003 will provide process oriented approach to successful implementation of ISMS in accordance with ISO/IEC 27001.

SAI

ACROSS TECHNOLOGY

ISO/IEC 27000:2009

ISO 27004 ISMS measurements

- Guidance & Advice to develop ISMS measurements standard = how to measure EFFECTIVENESS of ISMS implementations (processes & controls)
  - Performance targets, benchmarking …
    - What to measure
    - How to measure
    - When to measure
    - Where to measure
    - Who can measure
  - Awareness, incident handling, audit trail analysis, application and use of procedures, access control effectiveness …

SAI ACROSS TECHNOLOGY

ISO 27005 ISMS Risk Management

- Scope: guidelines for information security risk management. The approach described within International Standard supports the general concepts specified in ISO/IEC 27001.
- Purpose: provides guidance on implementing process oriented risk management approach to assist in satisfactorily implementing & fulfilling information security risk management requirements of ISO/IEC 27001.

SAI ACROSS TECHNOLOGY

ISO/IEC 27000:2009

ISO 27006 ISMS Certification Bodies

- *Requirements for bodies providing audit & certification of ISMS*
- Scope: requirements & guidance for bodies providing audit & ISMS certification in accordance with ISO/IEC 27001, in addition to requirements contained within ISO/IEC 17021.
- Primarily intended to support accreditation of certification bodies providing ISMS certification according to ISO/IEC 27001.
- Purpose: ISO/IEC 27006 supplements ISO/IEC 17021 in providing requirements by which certification organizations are accredited, thus permitting these organizations to provide compliance certifications consistently against requirements set forth in ISO/IEC 27001.

SAI ACROSS TECHNOLOGY

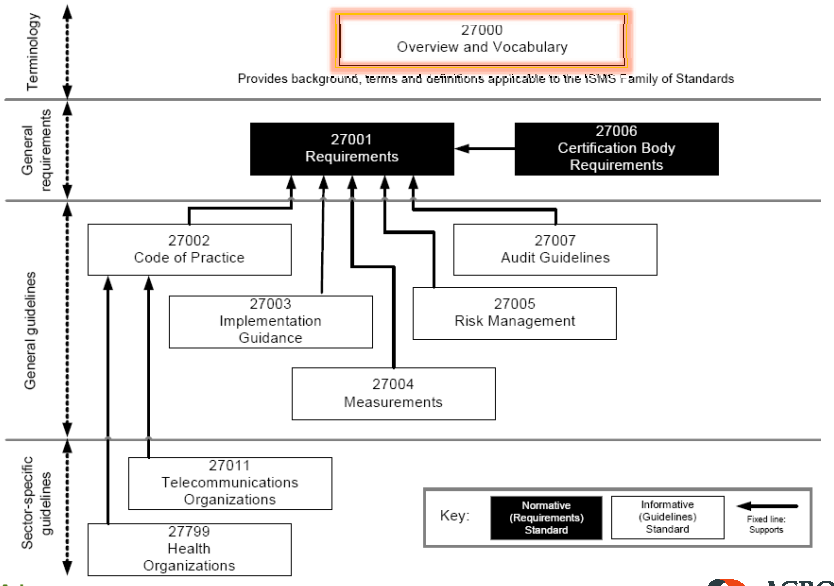
ISO 27007 ISMS auditing guidelines

- *Requirements for bodies providing audit & certification of ISMS*
- Scope: provide guidance on conducting ISMS audits, as well as guidance on the competence of information security management system auditors, in addition to the guidance contained in ISO 19011, which is applicable to managements systems in general.
- Purpose: ISO/IEC 27007 will provide guidance to organizations needing to conduct internal or external audits of an ISMS or to manage an ISMS audit programme against the requirements specified in ISO/IEC 27001.

SAI ACROSS TECHNOLOGY

ISO/IEC 27000:2009

ISO/IEC 27000:2009 Overview



SAI

ACROSS TECHNOLOGY

ISO/IEC 27000:2009

INTERNATIONAL STANDARD

ISO/IEC 27000

First edition
2009-05-01

Information technology — Security techniques — Information security management systems — Overview and vocabulary

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de la sécurité des informations — Vue d'ensemble et vocabulaire

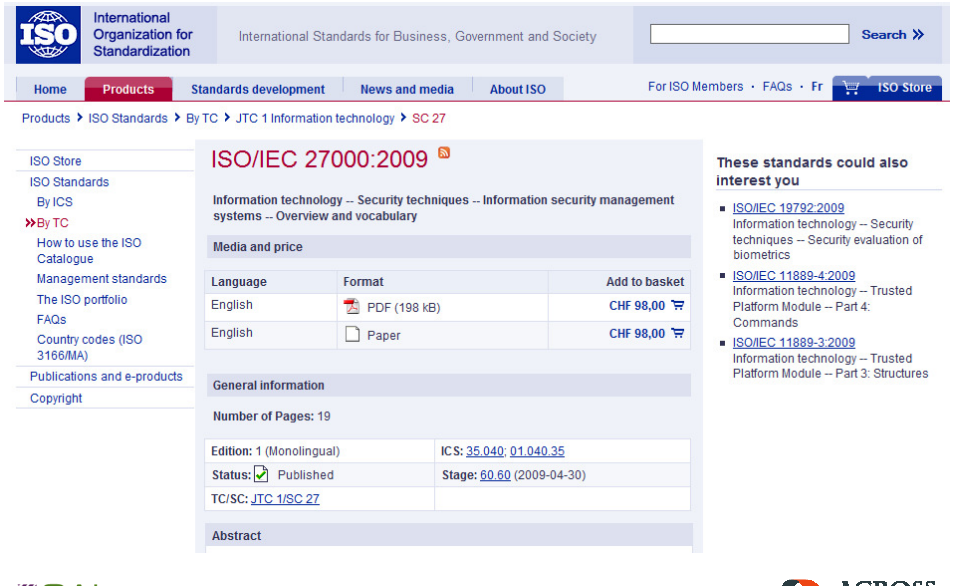
Reference number
ISO/IEC 27000:2009(E)

SAI

ACROSS TECHNOLOGY

ISO/IEC 27000:2009

ISO/IEC 27000:2009 cost



SAI

ACROSS TECHNOLOGY

ISO/IEC 27000:2009 table of contents

SAI

ACROSS TECHNOLOGY

ISO/IEC 27000:2009

Definitions

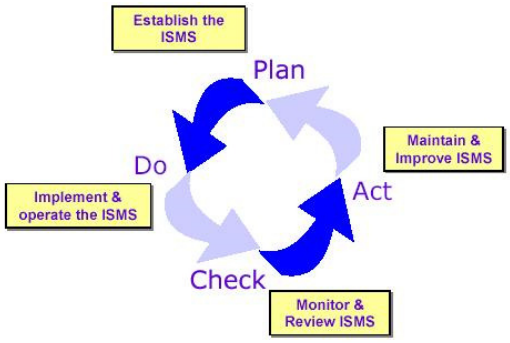
ISO/IEC 27000:2009

- International Standards for Management Systems
- Model to follow in setting up & operating an Information Security Management System (ISMS).
- Allow organizations
  - to develop & implement framework for managing security of their information assets
  - to prepare for independent assessment of their ISMS applied
    - to information protection (e.g. financial information, intellectual property, employee details)
    - to information entrusted to them by customers or third parties.

SAI ACROSS TECHNOLOGY

Purpose

- ISMS family of standards includes standards that:
  - define requirements for ISMS & for those certifying such systems;
  - provide direct support, detailed guidance and/or interpretation for overall Plan-Do-Check-Act (PDCA) processes & requirements;
  - address sector-specific guidelines for ISMS;
  - address conformity assessment for ISMS.



SAI ACROSS TECHNOLOGY

ISO/IEC 27000:2009

Purpose

- Applicable to all organization types (public, private, non-profit)
- Terms & Definitions provided in this standard:
  - cover commonly used terms & definitions in ISMS family of standards;
  - will not cover all terms & definitions applied within ISMS family of standards;
  - do not limit ISMS family of standards in defining terms for own use.

SAI ACROSS TECHNOLOGY

Terms & Definitions

B.1 Terms relating to information security

2.2 accountability
2.5 authentication
2.6 authenticity
2.7 availability
2.9 confidentiality
2.19 information security
2.25 integrity
2.27 non-repudiation
2.33 reliability

B.2 Terms relating to management

2.8 business continuity
2.12 corrective action
2.13 effectiveness
2.14 efficiency
2.16 guideline
2.23 information security management system (ISMS)
2.26 management system
2.28 policy
2.29 preventive action
2.31 process

SAI ACROSS TECHNOLOGY

ISO/IEC 27000:2009

Terms & Definitions

B.3 Terms relating to information security risk

2.1 access control
2.3 asset
2.4 attack
2.10 control
2.11 control objective
2.15 event
2.17 impact
2.18 information asset
2.20 information security event
2.21 information security incident
2.22 information security incident management
2.24 information security risk
2.34 risk
2.35 risk acceptance
2.36 risk analysis
2.37 risk assessment
2.38 risk communication
2.39 risk criteria
2.40 risk estimation
2.41 risk evaluation
2.42 risk management
2.43 risk treatment
2.45 threat
2.46 vulnerability

B.4 Terms relating to documentation

2.30 procedure
2.32 record
2.44 statement of applicability

SAI ACROSS TECHNOLOGY

Terms & Definitions

- **Access control:** means to ensure that access to assets is authorized & restricted based on business & security requirements
- **Accountability :** responsibility of an entity for its actions and decisions
- **Asset:** anything that has value to the organization
- **Attack:** attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset
- **Authentication:** provision of assurance that a claimed characteristic of an entity is correct
- **Authenticity:** property that an entity is what it claims to be
- **Confidentiality:** property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- **Control:** means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature
- **Effectiveness:** extent to which planned activities are realized and planned results achieved

SAI ACROSS TECHNOLOGY

ISO/IEC 27000:2009

Terms & Definitions

- **Efficiency:** relationship between the results achieved and how well the resources have been used
- **Guideline:** recommendation of what is expected to be done to achieve an objective
- **Impact:** adverse change to the level of business objectives achieved
- **Information asset:** knowledge or data that has value to the organization
- **Information security:** preservation of confidentiality, integrity and availability of information
- **Information security incident management:** processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents
- **ISMS:** part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
- **information security risk:** potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization
- **Integrity:** property of protecting the accuracy and completeness of assets

SAI studiecentrum voor automatische informatieverwerking vzw

ACROSS TECHNOLOGY

Terms & Definitions

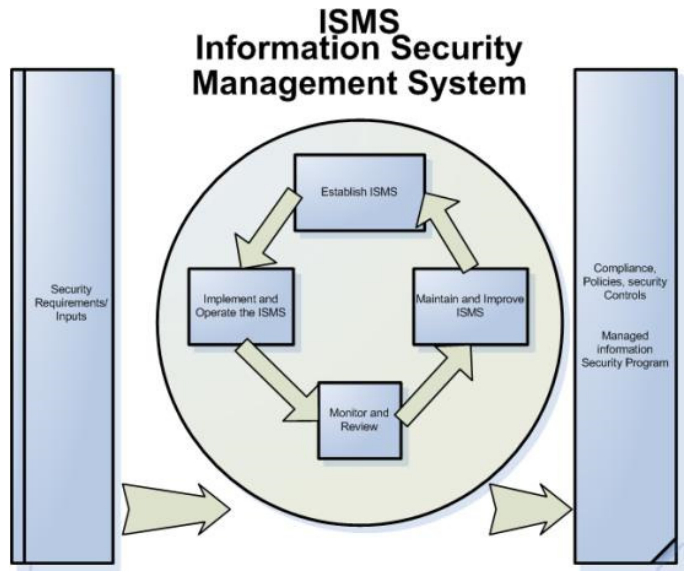
- **non-repudiation:** ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event
- **Policy:** overall intention and direction as formally expressed by management
- **Process:** set of interrelated or interacting activities which transforms inputs into outputs
- **Reliability:** property of consistent intended behaviour and results
- **Risk:** combination of the probability of an event and its consequence
- **Risk management:** coordinated activities to direct and control an organization with regard to risk
- **Risk treatment:** process of selection and implementation of measures to modify risk
- **Statement of Applicability:** documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS
- **Threat:** potential cause of an unwanted incident, which may result in harm to a system or organization
- **Vulnerability:** weakness of an **asset or control that can be exploited by a threat**

SAI studiecentrum voor automatische informatieverwerking vzw

ACROSS TECHNOLOGY

ISO/IEC 27000:2009

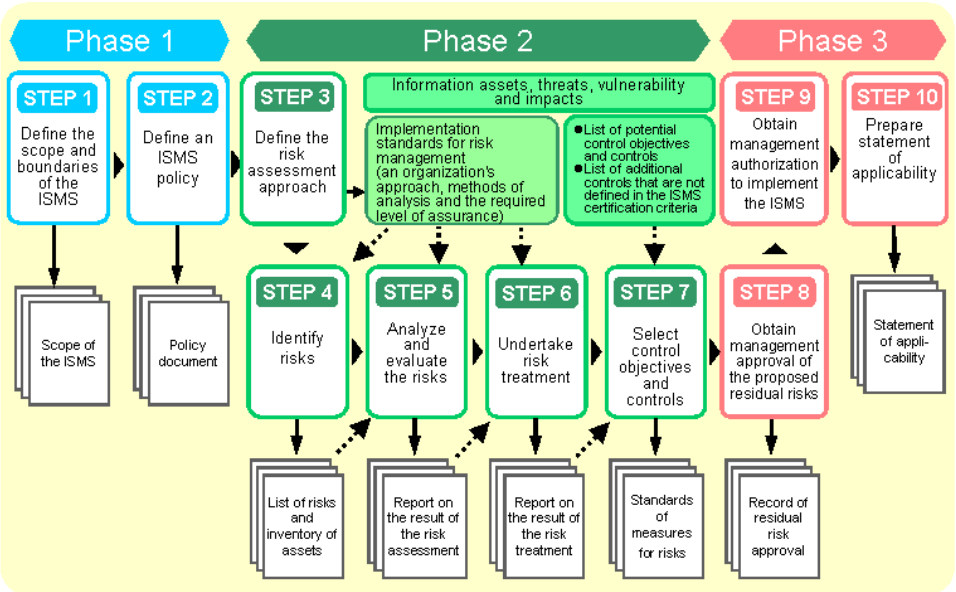
ISMS



SAI studiecentrum voor automatische informatieverwerking vzw

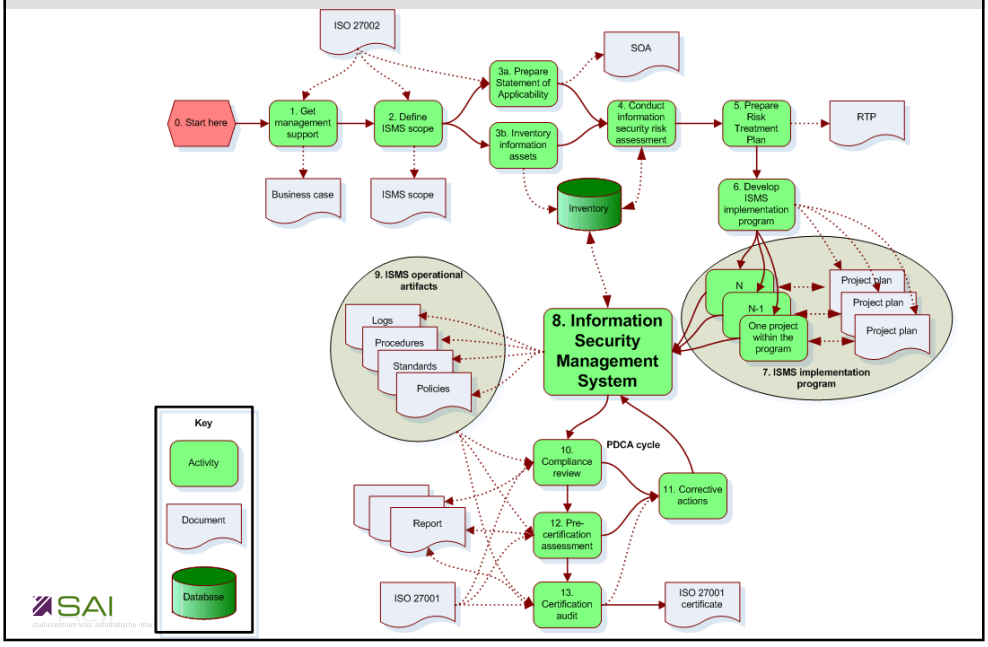
ACROSS TECHNOLOGY

ISMS



ISO/IEC 27000:2009

ISMS



ISMS

ISMS provides a model for

establishing, implementing, operating, monitoring, reviewing, maintaining and improving

the protection of information assets

to achieve business objectives

based upon risk assessment & organization's risk acceptance levels designed to effectively treat and manage risks.

ISO/IEC 27000:2009

ISMS

- Analysing requirements for protection of information assets & applying appropriate controls to ensure protection of these information assets, as required, contributes to successful implementation of ISMS.

SAI ACROSS TECHNOLOGY

ISMS

Following principles contribute to successful implementation of ISMS:

1. awareness of need for information security;
2. assignment of responsibility for information security;
3. incorporating management commitment & interests of stakeholders;
4. enhancing societal values;
5. risk assessments determining appropriate controls to reach acceptable levels of risk;
6. security incorporated as essential element of information networks & systems;
7. active prevention & detection of information security incidents;
8. ensuring a comprehensive approach to information security management;
9. continual reassessment of information security & making of modifications as appropriate.

SAI ACROSS TECHNOLOGY

ISO/IEC 27000:2009

Management System

- uses framework of resources to achieve organization's objectives.
- includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

In terms of information security, management system allows organization to:

1. satisfy security requirements of customers & other stakeholders;
2. improve organization's plans and activities;
3. meet organization's information security objectives;
4. comply with regulations, legislation and industry mandates;
5. manage information assets in organized way that facilitates continual improvement & adjustment to current organizational goals & environment.

SAI ACROSS TECHNOLOGY

ISMS CSF

1. information security policy, objectives, and activities aligned with objectives;
2. approach & framework for designing, implementing, monitoring, maintaining, and improving information security consistent with organizational culture;
3. visible support & commitment from all levels of management, especially top management;
4. understanding of information asset protection requirements achieved through application of information security risk management;
5. effective information security awareness, training and education program, informing all employees & other relevant parties of their information security obligations set forth in information security policies, standards etc., and motivating them to act accordingly;
6. effective information security incident management process;
7. effective business continuity management approach;
8. measurement system used to evaluate performance in information security management and feedback suggestions for improvement.

SAI ACROSS TECHNOLOGY

ISO/IEC 27000:2009

ISMS CSF

ISMS increases likelihood that an organization will consistently achieve critical success factors required to protect its information assets.

SAI ACROSS TECHNOLOGY

Why use ISMS?

Main benefit :
reduction in information security risks!

SAI ACROSS TECHNOLOGY

ISO/IEC 27000:2009

Why use ISMS?

- a) supporting process of specifying, implementing, operating and maintaining comprehensive & cost-effective integrated and aligned ISMS that meets organization's needs;
- b) assisting management in structuring their approach towards information security management, within context of corporate risk management & governance, including educating and training business & system owners on holistic management of information security

SAI ACROSS TECHNOLOGY

Why use ISMS?

- c) promoting globally-accepted good information security practices in non-prescriptive manner, giving organizations latitude to adopt and improve relevant controls that suit their specific circumstances and to maintain them in the face of internal & external changes;
- d) provising common language & conceptual basis for information security, making it easier to place confidence in business partners with compliant ISMS, especially if they require certification against ISO/IEC 27001 by accredited certification body.

SAI ACROSS TECHNOLOGY

ISO/IEC 27000:2009

Why Best Practices are Important!

Effective use of best practices can help

1. avoid re-inventing wheels,
2. optimize use of scarce IT resources
3. reduce occurrence of major IT risks, such as:
   - Project failures
   - Wasted investments
   - Security breaches
   - System crashes
   - Failures by service providers to understand & meet customer requirements

SAI ACROSS TECHNOLOGY

Why Best Practices are Important!

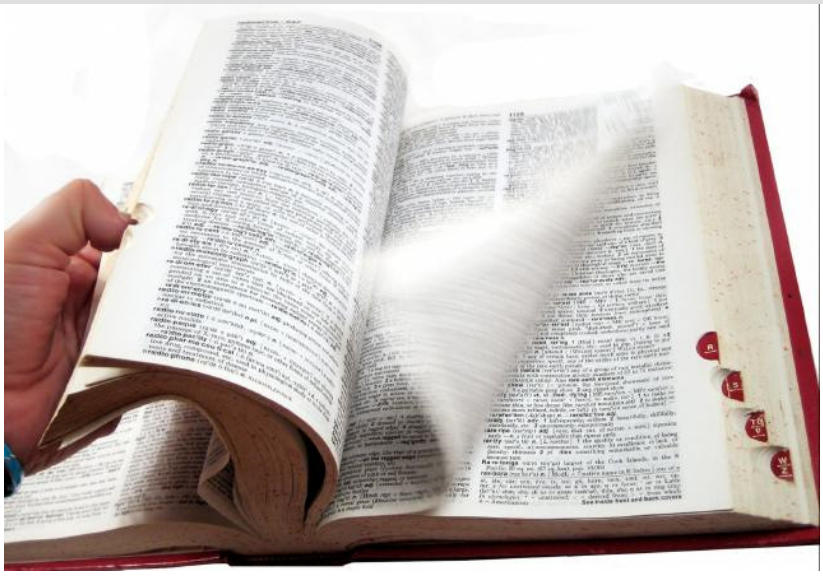
ISO 2700x = valuable to ongoing growth & success of any organization because:

1. Companies are demanding better returns from IT investments
2. Best practices help meet regulatory requirements for IT controls
3. Organizations face increasingly complex IT-related risks
4. Organizations can optimize costs by standardizing controls
5. Best practices help organizations assess how IT is performing
6. Management of IT is critical to success of enterprise strategy
7. Best practices help enable effective governance of IT activities
8. Management framework helps staff understand what to do (policy, internal controls and defined practices)
9. They can provide efficiency gains, less reliance on experts, fewer errors, increased trust from business partners and respect from regulators

SAI ACROSS TECHNOLOGY

ISO/IEC 27000:2009

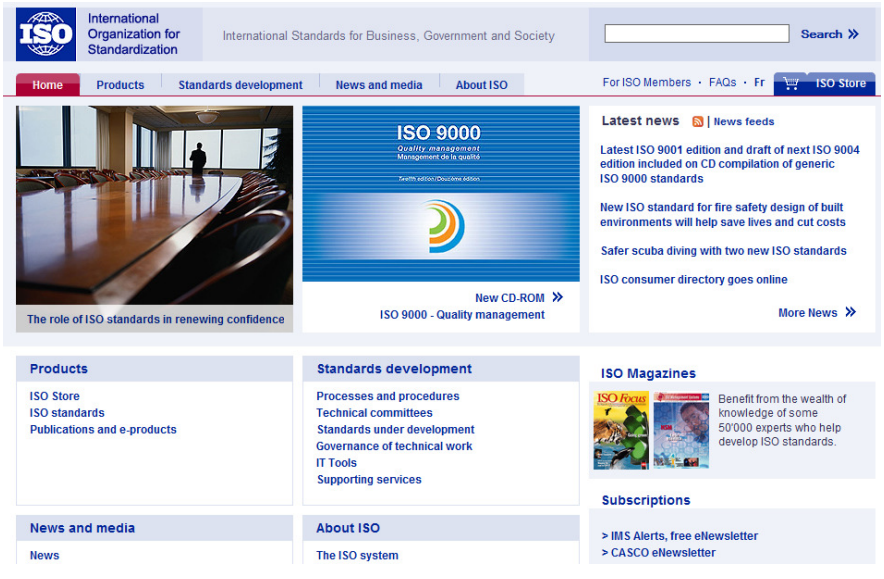
Conclusion



SAI studiecentrum voor automatische informatieverwerking vzw

ACROSS TECHNOLOGY

Relevant websites : www.iso.org



SAI studiecentrum voor automatische informatieverwerking vzw

ACROSS TECHNOLOGY

ISO/IEC 27000:2009

Other relevant websites around ISO/IEC 27000:2009

http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
http://www.standardsglossary.com
http://en.wikipedia.org/wiki/ISO_27000
http://www.27000-toolkit.com
http://www.praxiom.com/27001.htm
http://www.iso27001security.com/html/iso27k_toolkit.html
http://www.informationshield.com/iso17799.html

SAI
studiecentrum voor automatische informatieverwerking vzw

ACROSS TECHNOLOGY