Presentation on ISO/IEC 27001:2013

Information Security Management Systems (ISMS)

by John Njiri

Borasoft Ltd ... inspiring solutions.

IMPLEMENTATION OF INFORMTION SECURITY MANAGEMENT SYSTEMS (ISMS)

BASED ON ISO 27000 STANDARDS

TOP MANAGEMENT BRIEFING

Learning Objectives

- Introduce delegates to the concept of Information Security, Information Security Management Standards
- Understand Information Security as a PC requirement
- Delegates to understand requirements of Clause 5 of ISO/IEC 27001:2013 standard and how to implement them in the organization
- Give an overview of steps to certification

Information Security and Information Security Management

What is Information Security?

- Information Security is the preservation of Confidentiality, Integrity and Availability of information.
- In addition, other properties such as authenticity, accountability, non-repudiation and reliability should also be involved.

Why Information Security?

- The main aims include:-

  - ❖To ensure Business Continuity

  - ❖To minimize business damage by preventing and minimizing the impact of security incidents

C.I.A

Three basic components:

- **C — Confidentiality**

  The property that information is not made available or disclosed to unauthorized individuals, entities, or processes

- **I — Integrity**

  The property of safeguarding the accuracy and completeness of assets

- **A — Availability**

  The property of being accessible and usable upon demand by an authorized entity

  In some organizations integrity and/or availability may be more important than confidentiality.

What is ISMS?

- That part of the overall management system, based on a **business risk approach**, to establish, implement, operate, monitor, review, maintain and improve information security.
- A **management** process.
- Not a technological process.

ISO/IEC 27001:2013

Information Technology-Security Techniques – Information Security Management Systems – Requirements

Provides specific requirements;

- For establishing, implementing, maintaining and continually improving a documented ISMS designed to.
- For the assessment and treatment of information security risks tailored to the needs of the organization.

It is the only standard in the family used for certification

Types of Information

Internal

- Information that you would not want your competitors/ clients to know

Customer/client

- Information that they would not wish you to divulge

Shared

- Information that may be shared with other trading partners/ persons

Information Assets

In information security, computer security and network security an **Asset** is any data, device, or other component of the environment that **supports information - related activities**

Asset Examples

- **Information assets** – databases & data files, system documentation, user manuals, training materials, operational or support procedures, continuity plans, fall back arrangements.

- **paper documents –** contracts, guidelines, company documentation, documents containing important business results.

Asset Examples Cont...

- **Software assets –** application software, system software, development tools, utilities
- **Physical assets –** computer and communication equipment, magnetic media (tapes & discs), furniture (Cabinets, Safes, Desks & Drawers), etc.

Asset Examples Cont...

- **People –** personnel (full-time, part-time), customers, subscribers, suppliers.
- **Company image and reputation.**
- **Services –** computing and communicating services, other technical services (heating, lighting, power, air conditioning).

Asset Inventory

Inventory is drawn up of major assets

- Containing all major assets in ISMS
- Location
- Owner

(A.7.1.1)

Examples of information

- Commercial details (strategies, finances, business performance)
- Bids for contracts, market research reports
- Designs, patents, technical research, plans
- Passwords
- Personal details (health, credit rating, personal history, etc.)
- Names, addresses, phone numbers

Information lifecycle

Information may need protection through its entire lifecycle including deletion or disposal

- ✓ Create
- ✓ Store
- ✓ Distribute (to authorized persons)
- ✓ Modify (by authorized persons)
- ✓ Archive
- ✓ Delete (electronic) or Dispose (paper, disks etc.)

Risks, Threats & Vulnerabilities

Note: In Risk management, the ***Information Asset*** is what we are ***trying to protect***.

- ✓ **Threat** – A potential cause of an incident, that may result in harm of systems and organization. (*What we are trying to protect against*)
- ✓ **Vulnerability** – a **weakness of an asset** (resource) or a group of assets that can be exploited by one or more threats. (*The weakness or gap in our protection efforts*)
- ✓ **Risk** – effect of uncertainty on objectives. (*Intersection of assets, threats & vulnerabilities*)

Information Security Threats

- ✓ **Threat** – A potential cause of an incident, that may result in harm of systems and organization.

Threats can be classified according to their type and origin;

1) **Origin**: *Deliberate, Accidental, or Environmental.*
2) **Type**: *Physical, natural events, loss of essential services, compromise of information, technical failure, compromise of functions.*
3) **Human**: *Internal, External.*

Threats Classification - Origin

- ✓ Deliberate: aiming at information asset
  - ❖ spying
  - ❖ illegal processing of data
  - ❖ Intrusion of Systems
  - ❖ Masquerade
- ✓ Accidental
  - ❖ equipment failure
  - ❖ software failure
  - ❖ loss of power supply
- ✓ Environmental
  - ❖ natural event (Earthquake, fire, floods)

Threats Classification - Type

- ✓ Physical damage
  - ❖ fire
  - ❖ water
  - ❖ pollution
- ✓ natural events
  - ❖ climatic
  - ❖ Seismic
  - ❖ Volcanic
- ✓ loss of essential services
  - ❖ electrical power
  - ❖ air conditioning
  - ❖ Telecommunication
- ✓ technical failures
  - ❖ equipment
  - ❖ software
  - ❖ capacity saturation

Threats Classification – Type Cont…

- ✓ compromise of information
  - ❖ eavesdropping,
  - ❖ theft of media
  - ❖ retrieval of discarded materials

- ✓ compromise of functions
  - ❖ error in use
  - ❖ Intrusion of Systems
  - ❖ abuse of rights
  - ❖ denial of actions
  - ❖ Masquerade

Threats Classification - Human

- ✓ Internal
  - ❖ Angry Employees
  - ❖ Dishonest Employees
  - ❖ Criminals
- ✓ External
  - ❖ Governments
  - ❖ Terrorists
  - ❖ The Press
  - ❖ Hackers
  - ❖ Competitors

Information Security Vulnerability

- ✓ **Vulnerability** – a **weakness of an asset** (resource) or a group of assets that can be exploited by one or more threats

Examples:

Weak/ Broken Processes,

Ineffective Controls,

Weak Passwords,

Software bugs,

Hardware Flaws,

Business Change,

Human Ignorance.

Risks, Threats & Vulnerabilities

RISK is a function of **threats exploiting vulnerabilities** to obtain, damage or destroy assets.

Threats (actual, conceptual, or inherent) may exist, but if there are no vulnerabilities then there is **little/no risk**.

Similarly, you can have a vulnerability, but if you have no threat, then you have **little/no risk**.

Accurately assessing threats and identifying vulnerabilities is critical to understanding the risk to assets.

Risks, Threats & Vulnerabilities

RISK = Asset x Threat x Vulnerability

Example: In a system that allows weak passwords,

- Vulnerability – Weak Password is vulnerable to attacks or Hacking
- Threat - An intruder can exploit the password weakness to break into the system
- Risk - The resources within the system are prone to illegal access/ modification/ damage by the intruder.

Information Security Risks

✓ Examples of Information Security Risks:-

- Loss of Information
- Information theft
- Corruption of information/ Data
- Unauthorized access to information (Hacking, Whiteboards/ flipcharts)
- Denial of service
- Telephone conversations overheard
- Conversations overheard on public transport
- Access to Confidential information due to Social engineering

ISMS as a PC Requirement

Safety and Security Measures Indicator

- Implement the Information Security Management System (ISMS),

Step 1 (5%)

- Appoint ISMS leader –1%
- Appoint and train ISMS champions -2%
- Define scope -2%

Step 2 (5%)

- Brief top management on ISMS
- Train implementers – (process owners) – 2%
- Conduct awareness training for all employees – 2%

Step 3 (30%)

- Create ISMS Risk Management (Risk Registers and Risk Management Action Plan – 10%

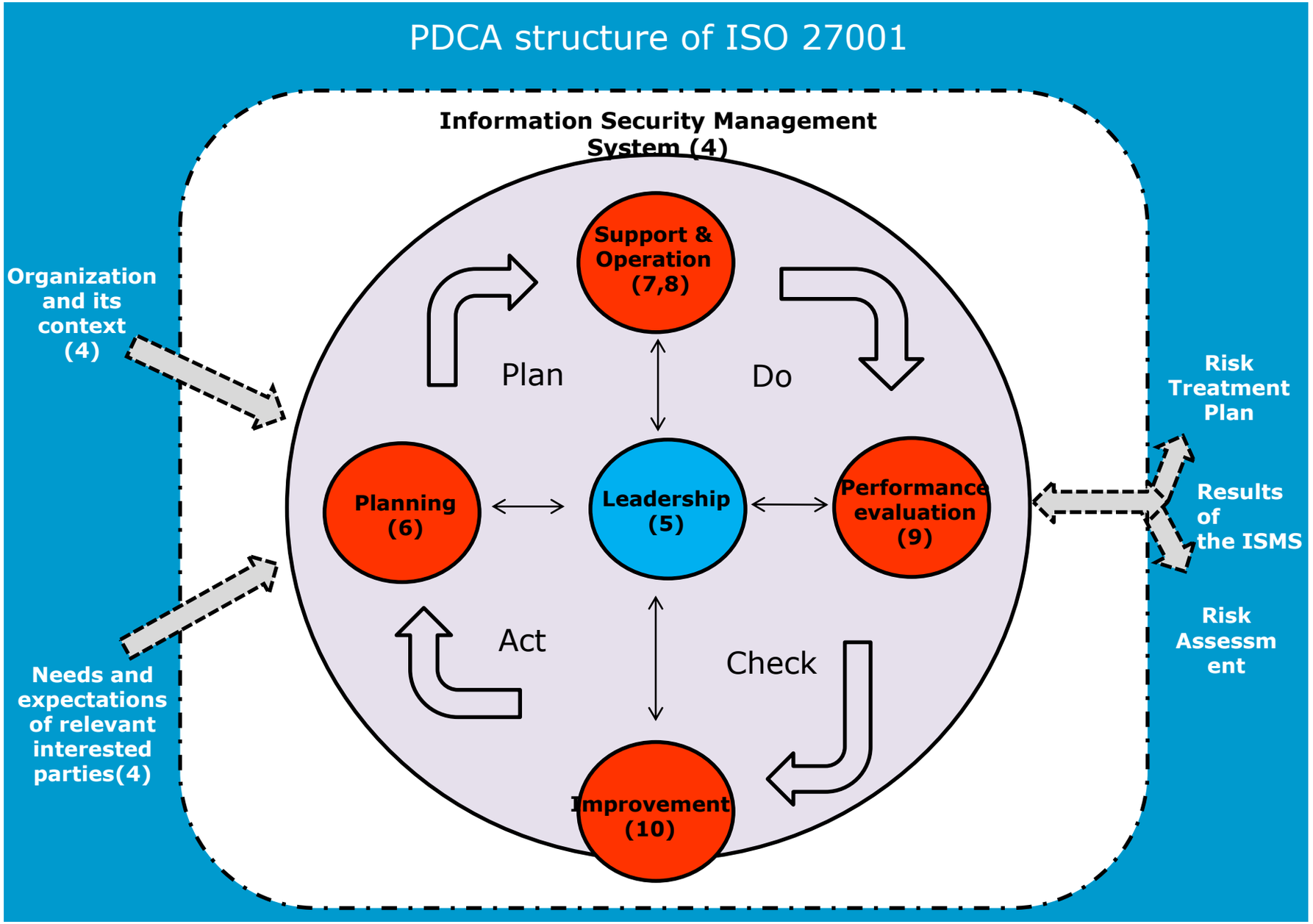
- Finalize documentation of ISMS i.e. policy procedures and launch the ISMS based on the standard (ISO/IEC) – 20%
- Establish information assets and secure them.(40%)

REQUIREMENTS OF ISO/ IEC 27001:2013 CLAUSE 5

Clauses within ISO 27001:2013

Clause 0: Introduction
Clause 1: Scope
Clause 2: Normative References
Clause 3: Terms and Definitions
Clause 4: Context of the Organization
Clause 5: Leadership
Clause 6: Planning
Clause 7: Support
Clause 8: Operation
Clause 9: Performance evaluation
Clause 10: Improvement
Annex A: Control objectives and Controls
Bibliography

PDCA Model applied to ISMS processes



Clause 5: Leadership

5.1 Leadership and commitment

- Top Managers are required to:-
  - ✓ensure that ISMS policy and ISMS objectives are established & are compatible to Company Strategy,
  - ✓ensure integration of ISMS requirements into processes,
  - ✓Ensure the resources required are available (Clause 7)

Clause 5: Leadership

5.1 Leadership and commitment

- Top Managers are required to:-
  - ✓communicating importance of effective information security management and of conforming requirements,
  - ✓ensure that ISMS achieves intended outcome,
  - ✓Promote continual improvement of the ISMS (Clause 10.2).

Clause 5: Leadership

5.1 Leadership and commitment

- Top Managers are required to:-
  - ✓motivate and empower employees,
  - ✓direct and supporting persons to contribute to the effectiveness of the information security management system, and
  - ✓support other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Clause 5: Leadership

5.2 Policy

- It is Top Management's documented commitment to satisfy applicable requirements related to IS,
- Should be periodically reviewed and revised to reflect changing conditions and information,
- Must be available to interested parties,
- All employees must be acquainted to the policy,

Clause 5: Leadership

5.2 Documentation requirements of the policy

The policy must:-

- be appropriate to the purpose of the organization;
- include information security objectives or provides a framework for setting IS objectives;
- include a commitment to satisfy applicable requirements related to IS; and
- include a commitment to continual improvement of the ISMS.

Clause 5: Leadership

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.

Clause 5: Leadership

5.3 Organizational roles, responsibilities and authorities

There is need to define the roles, responsibilities and authorities for:-

a) Top Management,

b) ISMS Manager,

c) ISMS Implementation Team,

d) ISMS Internal Auditors

e) Process Owners, and

f) Members of Staff.

Clause 5: Leadership

5.3 Organizational roles, responsibilities and authorities

a) Top Management

1. Development & review of ISMS policy,
2. Establishment, communication and monitoring of Information Security objectives,
3. Review, consider and approve information security policies and procedures,
4. Review, consider and approve the results of risk assessment,
5. Ensure availability of Resources for the ISMS.

Clause 5: Leadership

5.3 Organizational roles, responsibilities and authorities

b) ISMS Manager

1. Coordination and implementation of the ISMS policy and the supporting ISMS framework,
2. Maintaining the ISMS and ensuring its on-going conformity to ISO/IEC 27001
3. Supporting HODs & the ISMS implementation team by providing advice and guidance on all aspects of information security
4. Organizing and Managing internal ISMS Audits, & Reporting on the performance of the ISMS to the Managing Director.,
5. Planning and chairing ISMS Implementation team meetings.

Clause 5: Leadership

5.3 Organizational roles, responsibilities and authorities

c) Heads of Departments/ Process Owners

1. preservation of the confidentiality, integrity, and availability of information and information assets,
2. Conducting or facilitating of risk assessment and implementing risk treatments,
3. Noting and reporting information security weaknesses, information security events and identifying improvement opportunities;

Clause 5: Leadership

5.3 Organizational roles, responsibilities and authorities

c) Heads of Departments/ Process Owners (Cont...)

4. Responding to nonconformities by determining and implementing corrective actions;

5. Ensuring persons under their area of control are aware of the ISMS policy, their contribution to the effectiveness of the ISMS and the implications of not conforming to ISMS requirements.

9 Performance evaluation

9.3 Management review

Top management shall review the organization’s information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

STEPS TO CERTIFICATION

&

BENEFITS OF IMPLEMENTATION

Key Steps to Certification

1. Management Commitment/ Appoint ISMS Manager
2. Awareness Creation (Top, Implementers, Staff)
3. Define ISMS Scope and Policy
4. Document the ISMS (Policies, Procedures, etc.)
5. Undertake Risk Assessment &Treatment
6. Monitor Treatment Processes
7. Undertake internal Audits & Management Review
8. Undertake Pre-certification Audit
9. Certification Audits & corrective actions
10. Maintain Certification

Certification Assessment

Pre-assessment (optional)

Stage 1 — Documentation audit

Stage 2 — Implementation audit

Continuing surveillance

3-Year reassessment

Key Benefits of implementing ISO 27001

1. Compliance

Helps an organization comply to various regulations regarding data protection, privacy and IT or other information security governance.

2. Lowering the expenses

Financial gain if you lower your expenses caused by incidents, less interruption in service, or occasional data leakage, or disgruntled employees.

Key Benefits of implementing ISO 27001

3. Marketing edge

ISO/ IEC 27001 could be a unique selling point, especially if you handle clients' sensitive information.

4. Awareness

Greater Information security awareness within the organization

THANK YOU

Q&A

Muthaiga Suites, Opp. Oil Libya Plaza, Off Thika Super Highway
P.O. Box: 23158 - 00100 Nairobi, Kenya
Tel: +254 (0) 20 2629783/4, 722 507 360, 702 555 222
Email: info@borasoft.co.ke, njirijohn@borasoft.co.ke
Website: www.borasoft.co.ke