

Information Security Overview

Tim Ryan
Head of Sales, Management Systems
SAI Global

Some Questions

Is there anyone that has never heard of ISO Management Systems?

How many organizations certified to any ISO Management System Standard?

- Quality Management ISO 9001
- Environmental Management ISO 14001
- Aerospace AS 91XX

Are any organizations certified to ISMS ISO 27001

Agenda

- What are ISO Standards, Management Systems Standards (MSS), and the Information Security Management Systems (ISMS)
- Benefits of a MSS, particularly an ISMS
- Structure of Management Systems
- What is unique to ISMS
- Requirements particular to ISMS
- Questions and comments

What is a Management System Standard?

ISO Standards

ISO creates documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose

<https://www.iso.org/standards.html>

Management System Standards

ISO Management System Standards (MSS) help organizations improve their performance by:

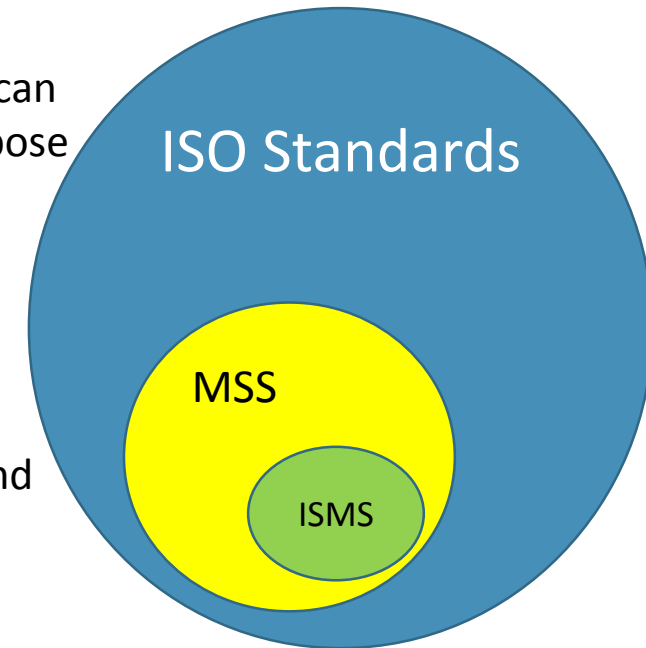
- Specifying repeatable steps consciously implemented to achieve their goals and objectives
- Creating a culture that reflexively engages in a continuous cycle of self-evaluation, correction, and improvement through heightened employee awareness and management leadership and commitment

<https://www.iso.org/management-system-standards.html>

Information Security Management System (ISMS)

An ISMS preserves the confidentiality, integrity and availability of Information by applying a risk management process and gives confidence to interested parties that risks are adequately managed

[ISO/IEC 27001:2013](#)



ISMS Benefits

- Reduces information security incidents
- Reduces risk of financial loss*
- Improves conformance and compliance to requirements*
- Protects brand and reputation*
- Gives confidence to interested parties*
- Increases competitive advantage*
- Improves consistency across an organization*



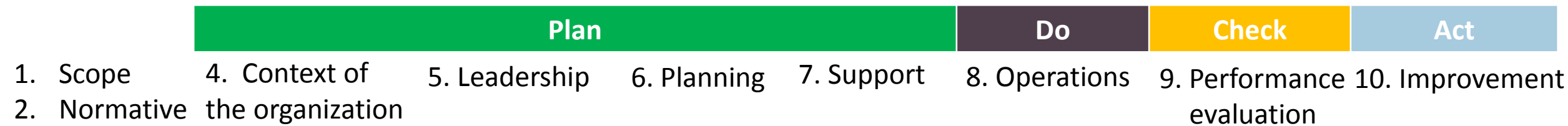
Financial Impacts

- Global average cost of a data breach is \$3.86m, +6.4% YoY
- Global cost for each lost or stolen record sensitive record \$148, +4.8% YoY
- Canada average breach cost \$4.7m
- US average breach cost \$7.9m

-Poneman Institute

*Common to all MMS

MSS Structure



2. Normative References
3. Terms and Definitions

Applicable to all MSS

Information Security Risk Assessment
Information security Risk Treatment

Information Security Risk Assessment
Information security Risk Treatment

Unique to ISMS



Within a defined scope of certification

ISMS Risk Assessment and Treatment

- Identify scope
- Identify Security Policy and Objectives
- Conduct Risk Assessment
- Document risk treatment plan- identify controls implemented and justify those not implemented
- Implement Risk Treatment Plan



ISMS Key Points

- The ISMS establishes, implements, maintains, and continually improves information security management, preserving the confidentiality, integrity, and availability of Information
- The ISMS is influenced by the organizations needs and objectives, security requirements, organizational processes, size, and structure
- The ISMS is part of and integrated with the organization's processes and management structure and will be considered in the design of processes, information systems, and controls

Questions or Comments

Thank you

Tim Ryan

Head of Sales, Management Systems

804-904-2366

tim.ryan@saiglobal.com