SOC Reporting vs. ISO 27001 Certification

Sumit Kalra, Practice Leader, Burr Pilger Mayer, Inc.

Core Competencies – C13

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Agenda

- SOC 2 Reporting Process
- ISO 27001 Certification Process
- Differences
- Testing Approach
- Miss-Conceptions
- Similarities
- Benefits
- References

SOC 2 Reporting Process

- Service Organization Control (SOC)
  - Internal control reports
  - Services provided by a service organization
  - Enable users to assess outsourced services risks
- Types of Report
  - SOC 1 – Relevant to User Entities' Internal Control over Financial Reporting
  - SOC 2 —Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
  - SOC 3 — Trust Services Report (SOC 2 Criteria)

SOC 2 Reporting Process

- Type I engagement:
  - Suitably designed
  - Placed in Operation
  - As of point in time
- Type II engagement:
  - Type I requirements
  - + Operating Effectively
  - Minimum 2 months

SOC 2 Reporting Process

User Organization

Outsourcing

SOC 2 Report

Service Organization

SOC 2 Report

Information

Information

SOC 2 Report

User Organization
Internal/External Auditor
& Regulatory Compliance

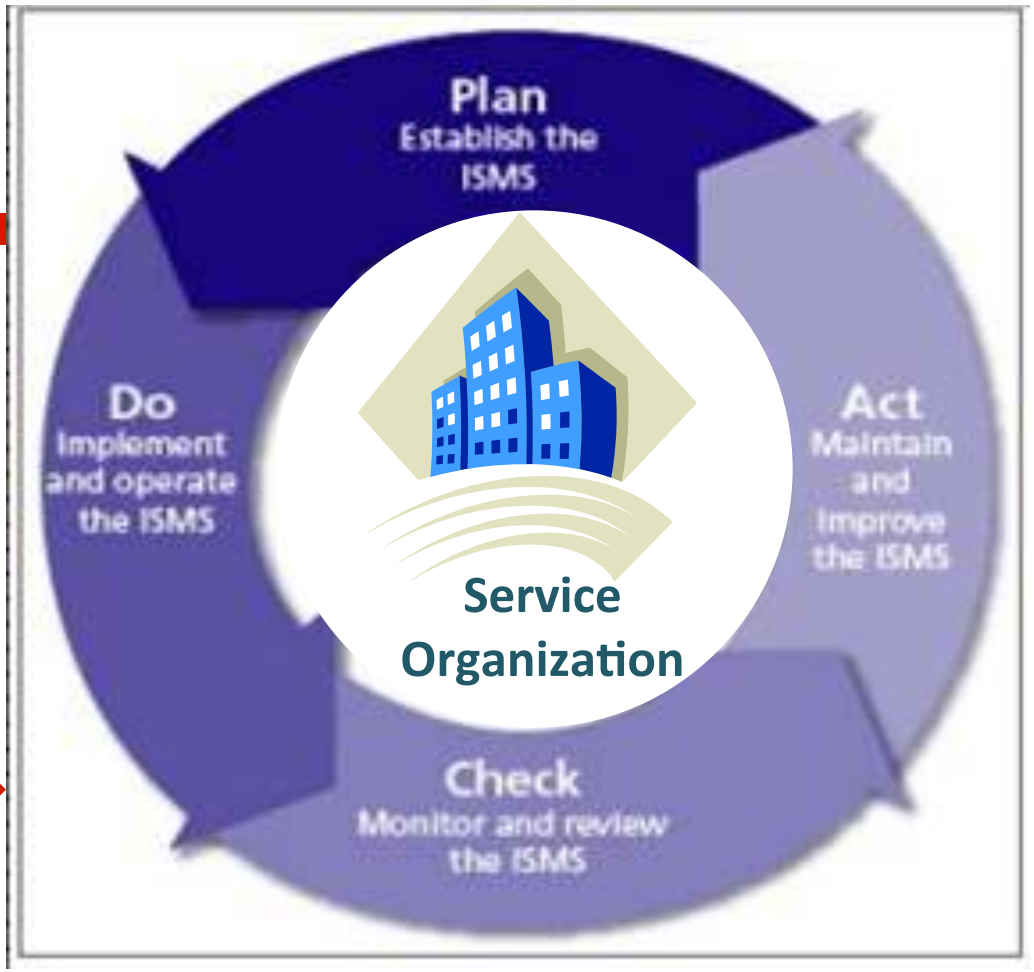
Service Organization
Auditor

ISO 27001 Certification Process

- Security Management System
- Demonstrates Explicit Management Control
- Mandates Specific Requirements
- Claim of Adoption Audited and certified

ISO 27001 Certification Process

Services



ISO 27001
Certification

Re-Certification

ISO 27001 Certification Process

- Oversight Body – ANAB
- Three Year Cycle
- 1st Year – Full Audit
  - Stage 1
  - Stage 2
- 3 Surveillance Audits
- 4th Year – Recertification (Full Audit)

Differences

SOC

- Examination
- AICPA
- Annual/Semi-Annual Cycle
- CPA Signed Opinion
- Skip Cycles

ISO

- Certification
- ANAB
- Certification Audit - 3 Surveillance Audits
- Recertification
- Cannot Skip Cycles

Differences

SOC

- Reports are issued with/without exceptions
- Internal Audits not a requirement
- Reports issued by Licensed CPA

ISO

- Conformity/Non-Conformity to the standard
- Required internal audits
- Certifications approved by ANAB

Testing Approach

SOC

- Controls based on Criteria
- All applicable controls every cycle
- Testing Covers Reporting Period
- May Leverage Internal Audit's work

ISO

- Management System based on ISO 27001
- Initial Full Audit – Two Stages
- Three Surveillance Audits
- Review of Internal Audit Required

Miss Conceptions

- We want to be Certified ----- ISO? SOC?
- We have controls in place ----- ISO? SOC?
- Which one is easier to get ---- ISO? SOC?
- I would like to push this out ---- ISO? SOC?
- Tell us what you want to see ---- ISO? SOC?
- We know the process is broken ---- ISO? SOC?
- We have one, I am ready for the other…
- Management just wants it done…

Similarities

- Assure management, Users and Other Stakeholders that relevant security risks are effectively managed.
- More or less covers aspects of Security, Availability, Confidentiality and Integrity.
- Neither one gives assurances that the organization follows the laws and regulation.

Benefits

- Audited only once by an independent auditor vs. being audited by management, stakeholders and customers.
- Achieve cost reduction through standardization of processes.
- Transparency with clients on compliance and audit results.
- Reduce sales cycle by significant number of days.

References

- AICPA
- ANAB

Questions

- ?????
- Sumit Kalra, IT Compliance and Assurance Services
- Skalra@bpmcpa.com
- 415-999-4553