AUDITING IN CONTEXT

Muryan Awaludin

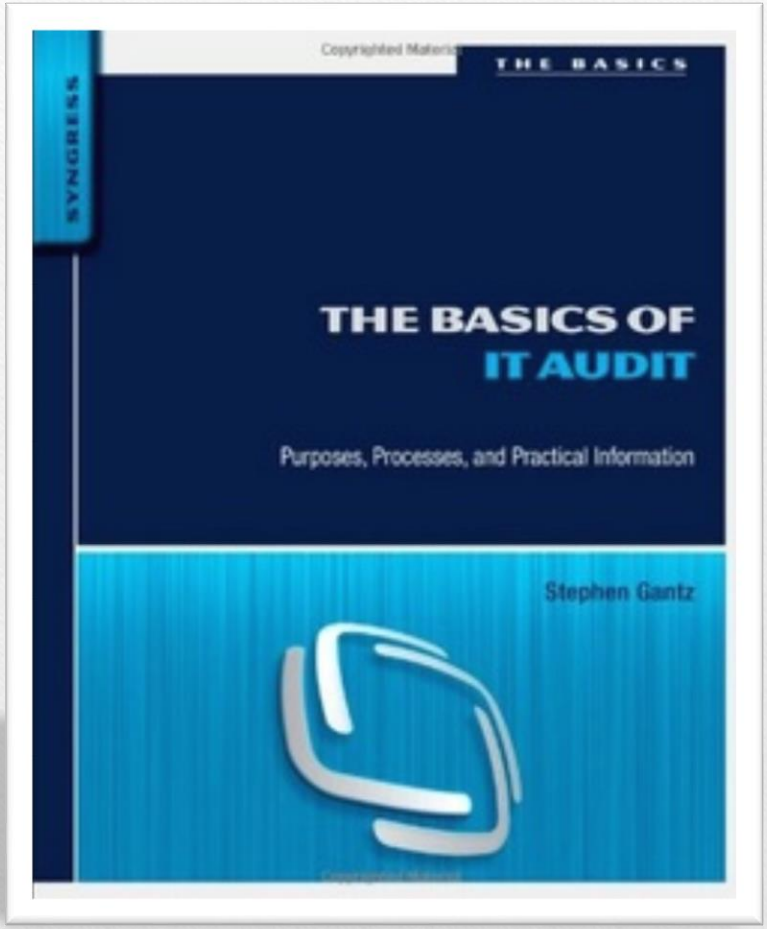
Muryan Awaludin

- SDN 09 Petarukan Pemalang (1997)
- SMP PGRI 5 Petarukan Pemalang (2000)
- SMK ISLAM Pemalang (2003)
- S.Kom di STIKOM CKI Jakarta (2010)
- M.Kom di STMIK ERESHA Jakarta (2014)

Contact

- Phone : 08562616116
- Email : muryan_awaludin@yahoo.co.id
- Blog : www.ilmudesaingrafis.blogspot.com
  : www.muryanawaludin.blogspot.com
- Twitter : @muryan_awaludin
- FB : muryan.awaludin
- Ym : muryan_awaludin

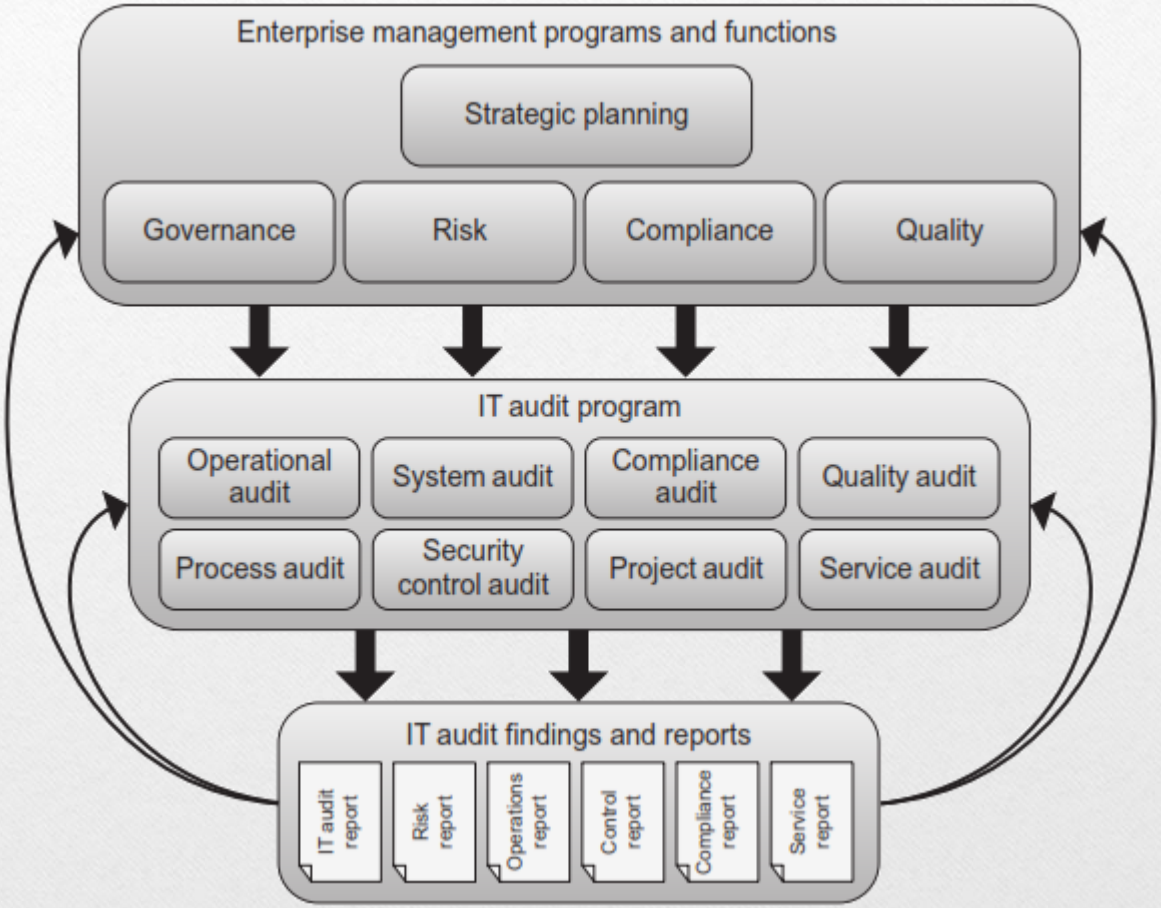
Textbooks


SYNGRESS
THE BASICS
THE BASICS OF
IT AUDIT
Purposes, Processes, and Practical Information
Stephen Gantz

Course outline

1. IT Governance
2. Risk Management
3. Compliance and certification
4. Quality Management and Quality Assurance
5. Information Security Management

Overview

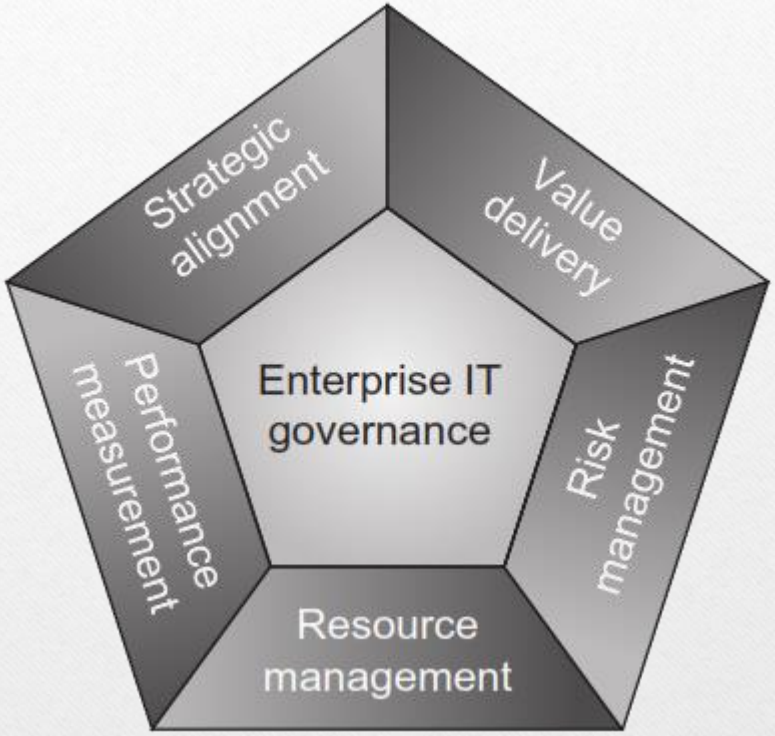

Enterprise management programs and functions
Strategic planning
Governance
Risk
Compliance
Quality
IT audit program
Operational audit
System audit
Compliance audit
Quality audit
Process audit
Security control audit
Project audit
Service audit
IT audit findings and reports
IT audit report
Risk report
Operations report
Control report
Compliance report
Service report

1. IT Governance

1. IT Governance

- **The term governance** in business contexts refers generally to the set of policies, processes, and actions taken by management to define organizational strategy and operate the organization in a way intended to help realize its business goals and objectives

1. IT Governance



The scope of IT governance *comprises* five key focus areas, each supported by well-defined processes and sets of internal controls [2].

1. IT Governance

As implemented in practice, IT governance comprises a wide range of processes and controls for applications, systems, networks, infrastructure, personnel, and data centers and other facilities**, including:**

- IT-related policies;
- standard operating procedures;
- management plans;
- performance monitoring and management;
- supervisory or oversight functions;
- IT controls and control monitoring;
- system and software development processes; and
- operations and maintenance activities.

1. IT Governance

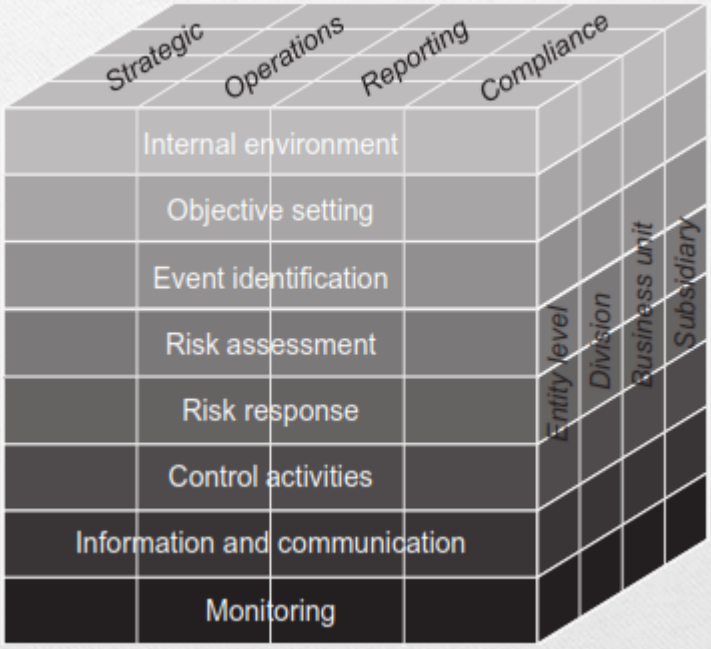
Sources of governance guidance focused on different organizational aspects below the enterprise level include:

- The Information Technology Infrastructure Library (ITIL) and ISO/IEC 20000 for service management;
- The Project Management Body of Knowledge (PMBOK) and Projects in Controlled Environments version 2 (PRINCE2) for project management;
- Capability Maturity Model Integration (CMMI) and ISO/IEC 15504 for software development processes; and
- The ISO/IEC 27000 series and National Institute of Standards and Technology (NIST) risk management framework for information security management.

2. Risk Management

2. Risk Management

All organizations have some exposure to risk the potential for loss, damage, injury, or other undesirable outcome resulting from decisions, actions, or events



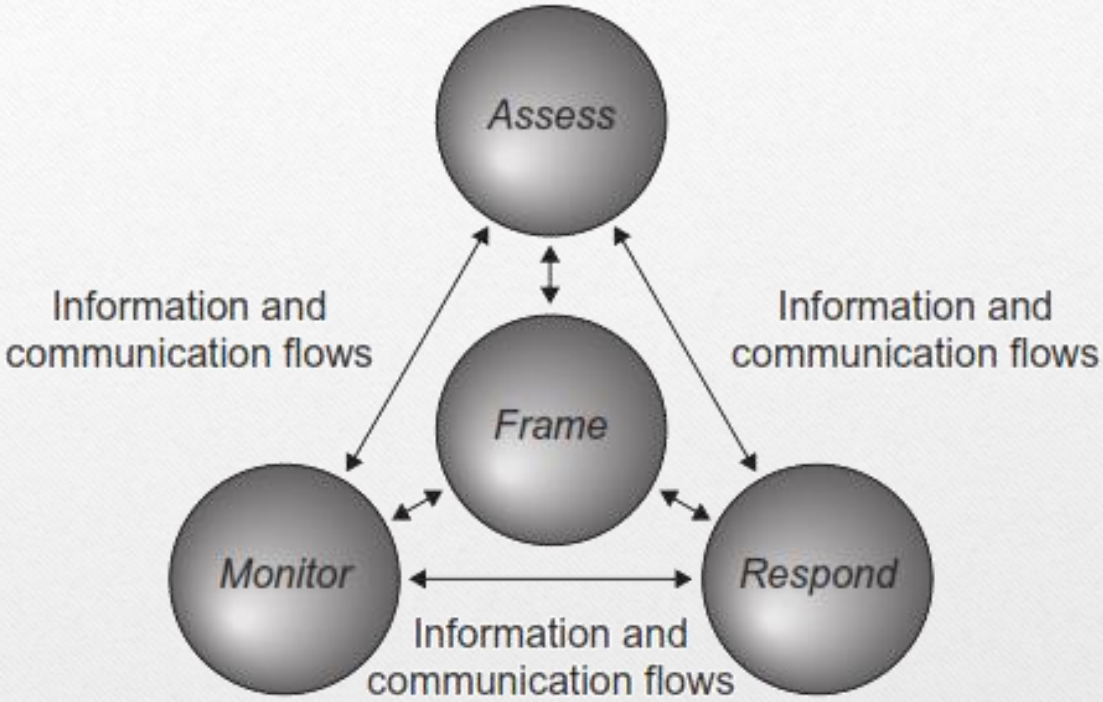
Source: Enterprise Risk Management—Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, ©2004. All rights reserved. Used by permission.

2. Risk Management

Risk Management Components

- The strategy specifies strategic planning assumptions, constraints, decision making criteria, and other factors influencing risk management in the organization, including the use of risk identification and evaluation procedures such as those associated with IT audit functions
- Once defined, organizations implement their risk management plans using an iterative cycle of processes and procedures, typically including risk identification, evaluation, response, monitoring, and review

2. Risk Management



NIST's risk management framework is a representative example of processes and methodologies that address specific types of risk, such as risk associated with operating information systems [6].

2. Risk Management

The role of IT audit in risk management

- IT auditing has both dependent and supporting roles within risk management
- The results of risk management activities influence the way the IT audit program plans results of risk management activities and audits, and the findings and recommendations from IT audits represent important inputs into assessment, and response

3. Compliance and certification

3. Compliance and certification

- **Compliance activities**

Aktivitas yang mempertimbangkan semua persyaratan yang berlaku untuk organisasi dan menilai sejauh mana organisasi memenuhi persyaratan, mengidentifikasi kesenjangan atau kegagalan untuk memenuhi persyaratan yang mungkin ada

- **Certification** is a special type of compliance. To achieve certification, organizations typically adopt standard processes or methodologies in a specifically prescribed manner

3. Compliance and certification

Managing compliance and certification

- Managing compliance and certification is an ongoing process
- Dibuktikan dengan adanya pengakuan dari pihak luar yang berwenang, serta dibatasi degan waktu atau frekuensi pemeriksaan yang diperlukan

3. Compliance and certification

Types of Organizational Certifications and Standards

Certification Focus	Certifications
Quality management	• ISO 9001 • ISO 14001
Information security management	• ISO/IEC 27001 • Cybertrust
Service management	• CMMI for services • ISO/IEC 20000
Service organization controls	• SSAE 16 • ISAE 3402 • SOC 2 and 3
Process improvement	• CMMI • ISO/IEC 15504 • Six Sigma
Products or technologies	• Common criteria • CESG assisted products scheme (United Kingdom) • FIPS (United States)

3. Compliance and certification

The role of IT audit in compliance and certification

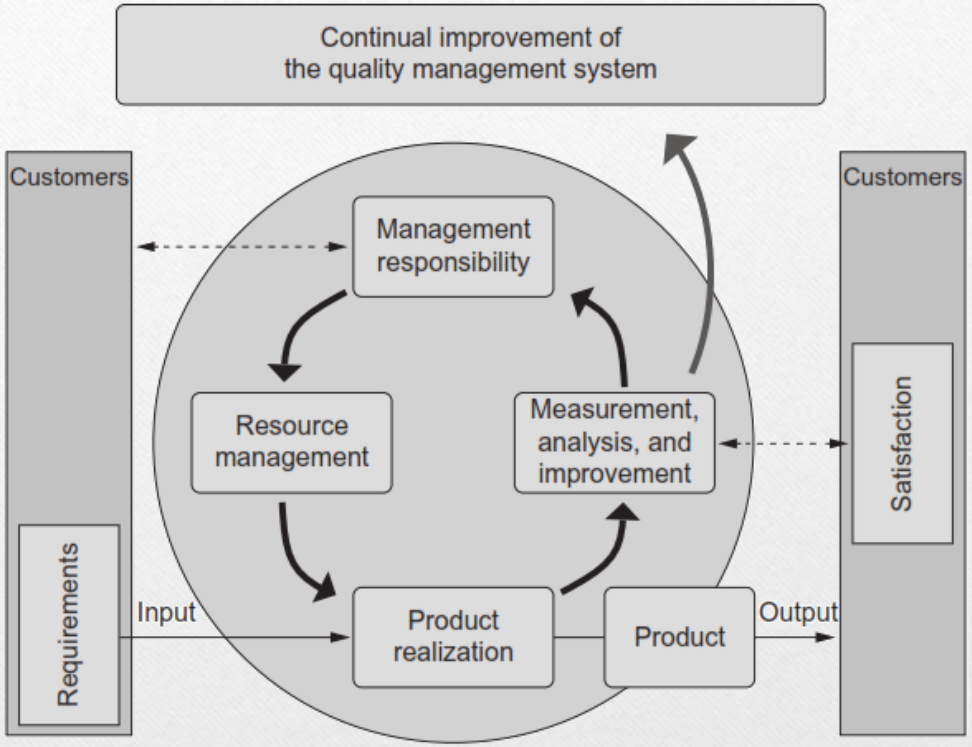
The central role of IT auditing in organizational compliance and certification is compare organizational behavior or operational characteristics to explicit sets of requirements

4. Quality management and quality assurance

4. Quality management and quality assurance

Quality assurance mengacu pada proses yang terkait dengan pencapaian dan mempertahankan tingkat kualitas yang diinginkan dalam suatu produk atau jasa

4. Quality management and quality assurance



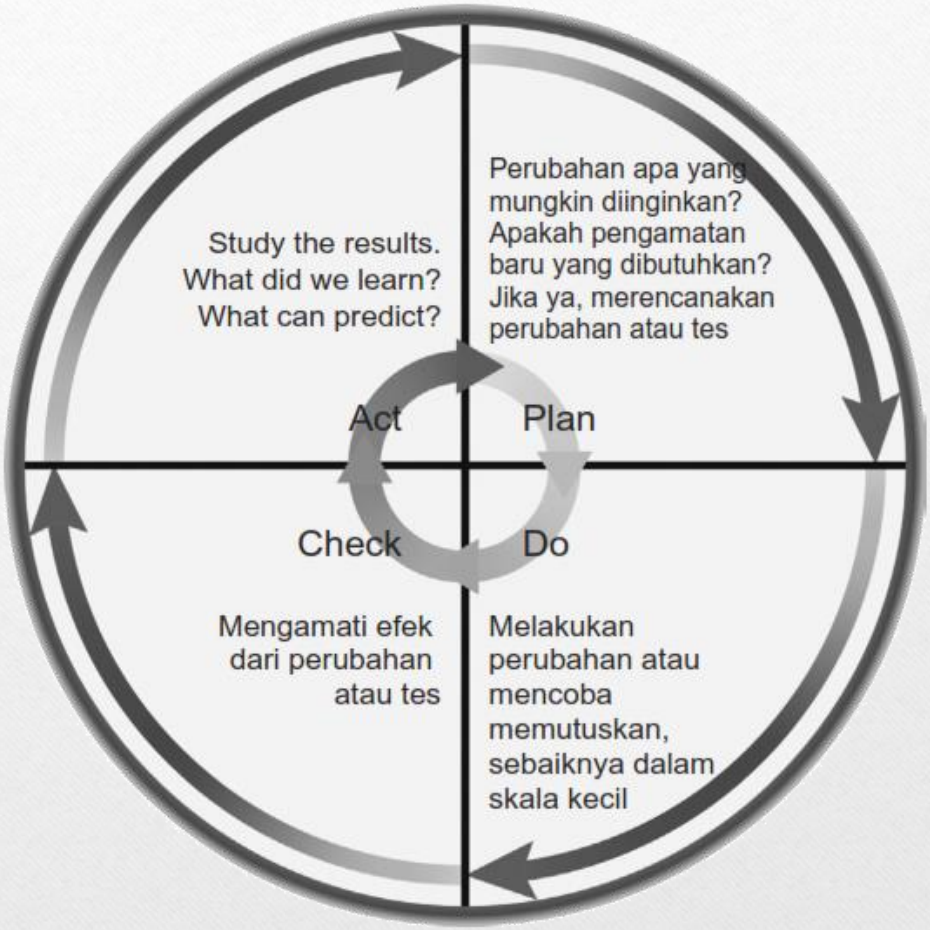
The process defined in ISO 9001 uses an iterative approach and emphasizes the continuous improvement characteristic of quality management systems [21].

4. Quality management and quality assurance

The contributions of quality management on the field of IT auditing go far beyond the use of audit procedures in quality assurance activities

As the processes specified in many governance, risk management, service management, and auditing methodologies share a common foundation in the plan-do-check-act (PDCA) cyclical model generally attributed to W. Edwards Deming (the "Deming cycle")

4. Quality management and quality assurance



The PDCA cycle popularized by W. Edwards Deming arose out of quality management but is widely used in other management domains including IT governance, information security, risk management, and auditing [23]

4. Quality management and quality assurance

The role of IT audit in quality management

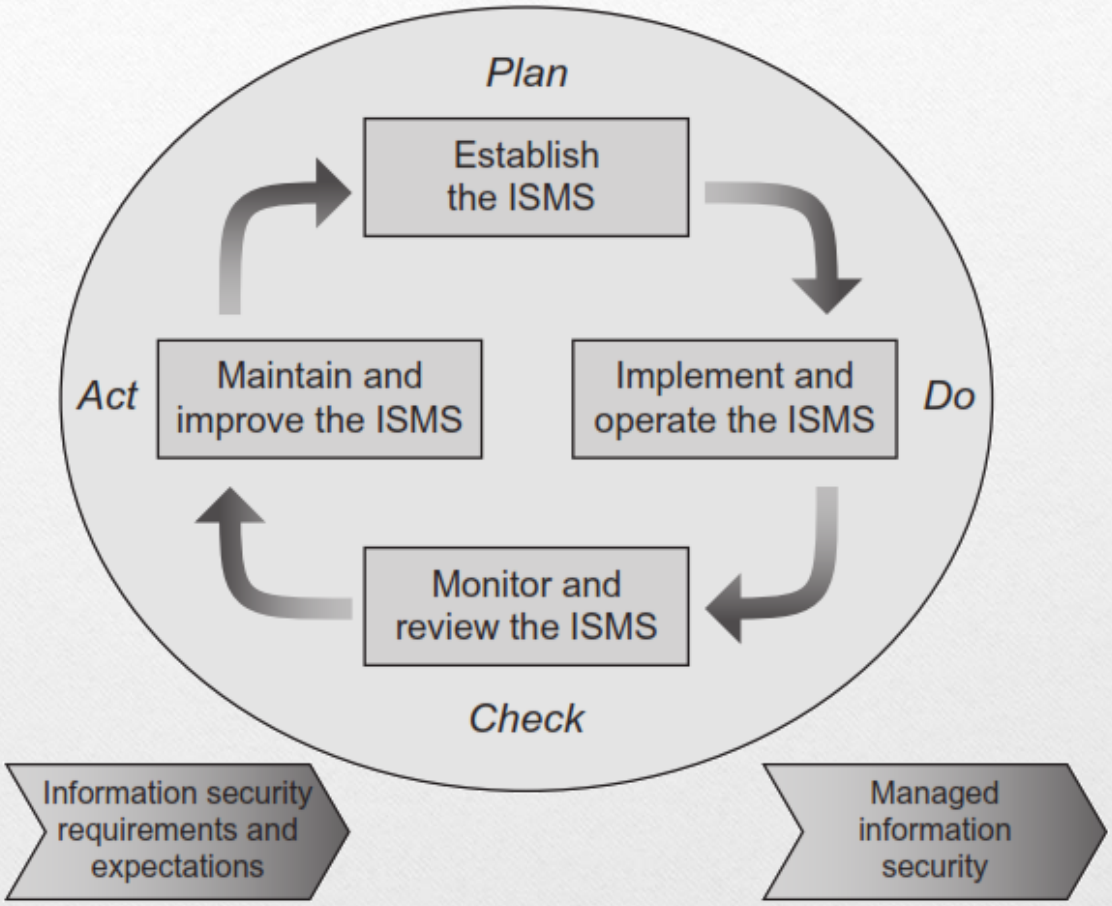
- IT audit mendukung fungsi manajemen mutu organisasi, dengan mengkonfirmasi bahwa proses operasional menghasilkan hasil yang diinginkan dan bahwa output dari proses-proses tersebut memenuhi kriteria kualitas yang berhubungan
- Sistem manajemen mutu juga dikenakan pemeriksaan berkala untuk menentukan apakah sistem seperti yang diterapkan memenuhi persyaratan yang berlaku

5. Information security management

5. Information security management

- Information security is often considered a subordinate function to IT governance, risk management, or both, and in t hat respect differs from the other management
- Information security management entails the selection, implementation, configuration, operation, and monitoring of security controls sufficient to protect the confidentiality, integrity, and availability of information systems and the data they contain

5. Information security management



The ISMS process defined in ISO/IEC 27001 applies the familiar PDCA model to information security management [26].

5. Information security management

The role of IT audit in information security management

- Information security management supports IT auditing by taking responsibility for implementing and correctly configuring internal controls related to security
- Security controls are an important subject of internal controls, but still a subset, meaning information security does not cover the full range of IT controls in an organization

Relevant source material

Key sources of additional information include:

IT governance

- Control Objectives for Information and Related Technology (COBIT) [3]
- COSO's Internal Control—Integrated Framework [29]
- ISO/IEC 38500:2008, Corporate Governance of Information Technology [30]
- Web sites and online resources of the IT Governance Institute (http://www. itgi.org) and ISACA (http://www.isaca.org)

Risk management

- Coco's Enterprise Risk Management—Integrated Framework [10]
- ISO/IEC 31000:2009, Risk Management—Principles and Guidelines [5]
- NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View [6]

Compliance and certification

- Statement on Auditing Standards 117, Compliance Audits [17]
- ISO online guidance on certification [31] and standards and guidance from the ISO Committee on Conformity Assessment (CASCO)

Quality management

- The ASQ Auditing Handbook [22]
- ISO 9001:2008, Quality Management Systems—Requirements [21]
- IAASB Handbook of International Quality Control, Auditing Review, Other Assurance, and Related Services Pronouncements[32]

Information security management

- ISO/IEC 27001:2005, Information—Security Techniques—Information Security Management Systems—Requirements[26]
- ISO/IEC 27002:2005, Information Technology—Security Techniques—Code of Practice for Information Security Management[33]
- NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations[34]

Thank You

Next --->

REFERENCES

[1] IT Governance Institute Board briefing on IT governance, 2nd ed Rolling Meadows (IL): IT Governance Institute; 2003.

[2] IT Governance Institute CobiT 4.1. Rolling Meadows (IL): IT Governance Institute; 2007.

[3] ISACA COBIT 5: a business framework for the governance and management of enter- prise IT. Rolling Meadows (IL): ISACA; 2012.

[4] ISO Guide 73:2009. Risk management—Vocabulary.

[5] ISO/IEC 31000:2009. Risk management—Principles and guidelines.

[6] National Institute of Standards and Technology Managing information security risk:

REFERENCES

[7] Wrightson MT, Caldwell SL. Further refinements needed to assess risks and prioritize protective measures at ports and other critical infrastructure. Report to Congressional

[8] Crouhy M, Galai D, Mark R. The essentials of risk management. New York (NY): McGraw-Hill; 2006.

[9] ISO/IEC 27005:2011. Information technology—Security techniques—Information security risk management.

[10] Committee of Sponsoring Organizations of the Treadway Commission Enterprise risk management—Integrated framework. New York (NY): Committee of Sponsoring Organizations of the Treadway Commission; 2004.

[11] Common Vulnerabilities and Exposures [Internet]. McLean (VA): The MITRE Corporation [updated 2013 May 16; cited 2013 June 4].

[12] CERT Coordination Center [Internet]. Pittsburgh (PA): Software Engineering Institute [cited 2013 June 4

REFERENCES

[13] US-CERT—United States Computer Emergency Readiness Team [Internet]. Washington (DC): Department of Homeland Security [cited 2012 January 15].

[14] International Organisation of Supreme Audit Institutions Information system security review methodology. Copenhagen (DK): INTOSAI Professional Standards Committee; 1995. [ISSAI 5310. Appendix H].

[15] Guide for conducting risk assessments. Gaithersburg (MD): National Institute of Standards and Technology, Computer Security Division; 2012 September.

[16] Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226 § 13411.

[17] Compliance audits. New York (NY): American Institute of Certified Public Accountants, Auditing Standards Board; 2009 December

REFERENCES

[18] ISO 9000:2005. Quality management—Fundamentals and vocabulary.

[19] IEEE P730-2002 Standard for software quality assurance processes. New York (NY):

[18] Securities and Exchange Commission. Management's report on internal control over financial reporting and certification of disclosure in Exchange Act periodic reports; final rule. 68 Fed. Reg. 36636; 2003.