Universitas Komputer Indonesia

IT Audit and Control

Dr. Yeffry Handoko Putra, M.T

MAGISTER SISTEM INFORMASI

Sylabus

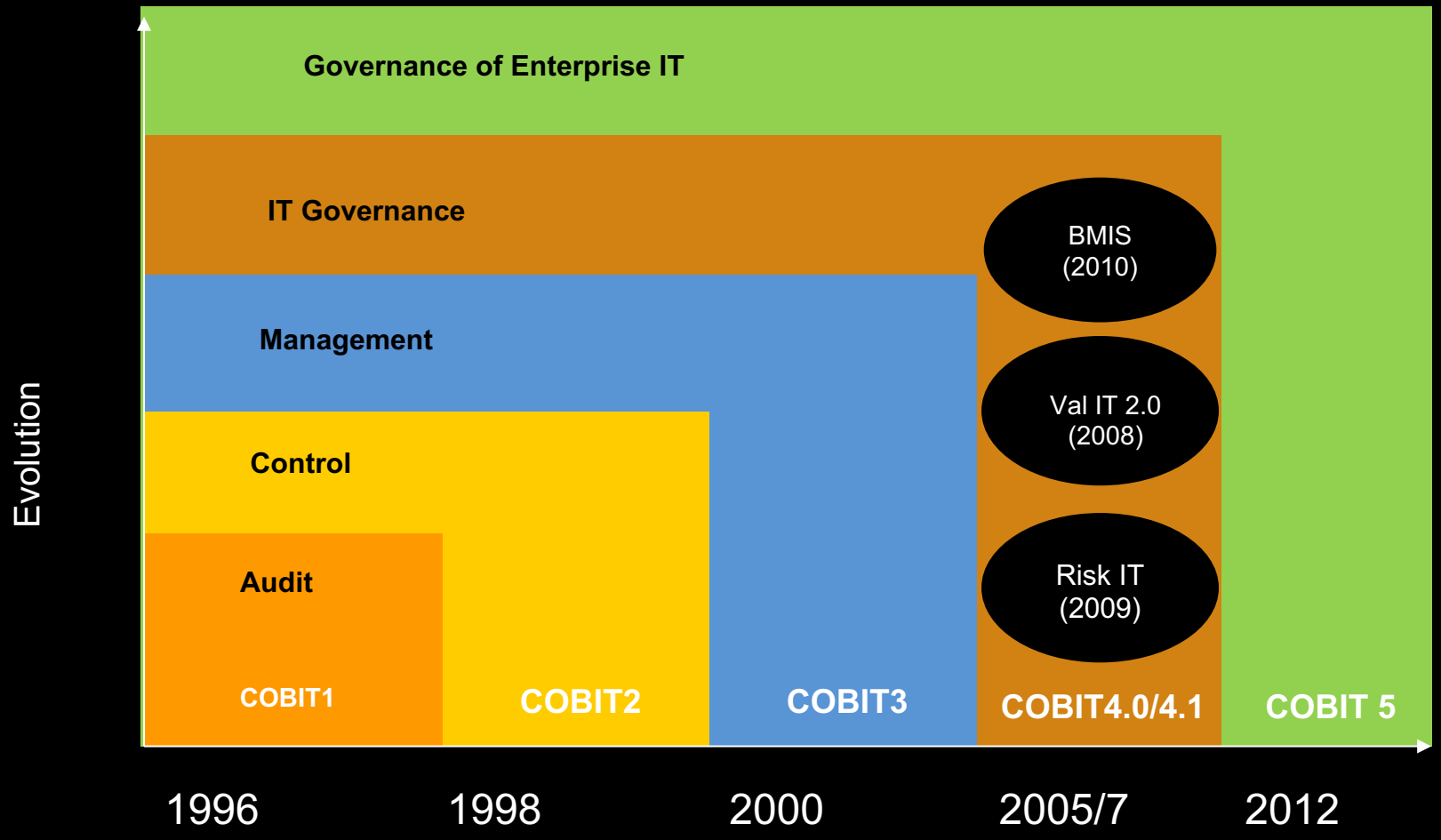
- Chap 1 – IT Audit Fundamental
- Chap 2 - Audit in Context
- Chap 3 – Internal Audit
- Chap 4 – External Audit
- Chap 5 – Audit Type and IT Audit Component
- Chap 6 - IT Audit Driver
- Chap 7 – IT Audit with COBIT 5
- Chap 8 – CISA Certification Review

Reference

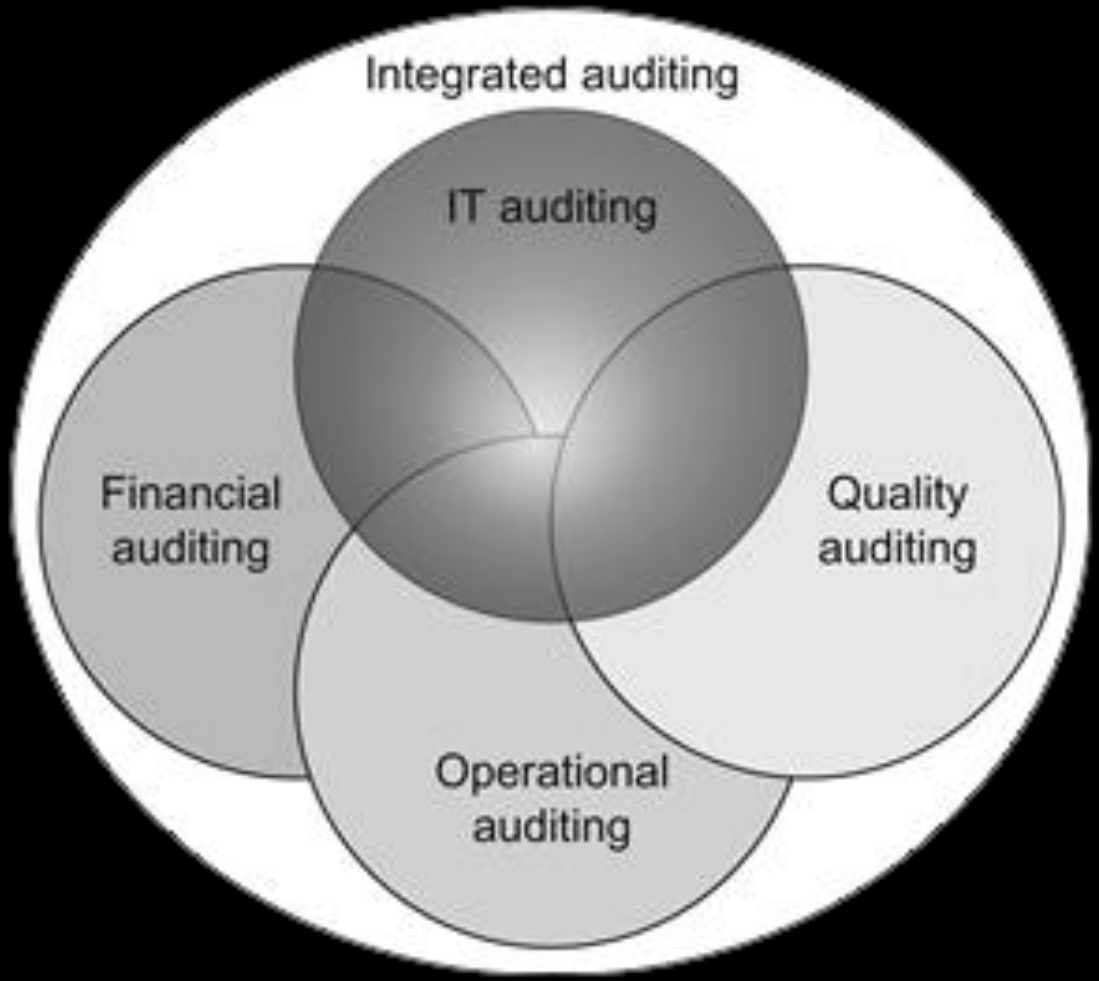
[Gantz] Gants, S.,(2014), The Basic of IT Audit, Elsevier

[ISACA] ISACA (2013), CISA Review Manual 2013

The Evolution of COBIT 5



Audit in many area



What is IT Auditing?

- Evaluating criteria conformity: ITIL
- Assessment :
  - Quantitative : Balanced Score Card: maturity model (cobit 4.1)
  - Qualitative : PAM Cobit 5 (e.g. Partially, Not available, Fulfilled)
- Inspection : CMMI model
- Comparing to standard, framework, requirement

What to audit

- entire organizations
- individual business units
- mission functions and business processes
- Services
- Systems
- Infrastructure
- or technology components

Focused on : controlling, finding bias (differentiation to standard), method

Who make IT audit?

- Internal Audit
- External Audit

Why should do IT Auditing?

- Preventive
- Correcting
- Detective

Some reason to do IT Auditing

- complying with securities exchange rules that companies have an internal audit function;
- valuating the effectiveness of implemented controls;
- confirming adherence to internal policies, processes, and procedures;
- checking conformity to IT governance or control frameworks and standards;

Some reason to do IT Auditing (2)

- analyzing vulnerabilities and configuration settings to support continuous monitoring;
- identifying weaknesses and deficiencies as part of initial or ongoing risk management;
- measuring performance against quality benchmarks or service level agreements;
- verifying and validating systems engineering or IT project management practices;

Who perform IT Auditing (The Actor)

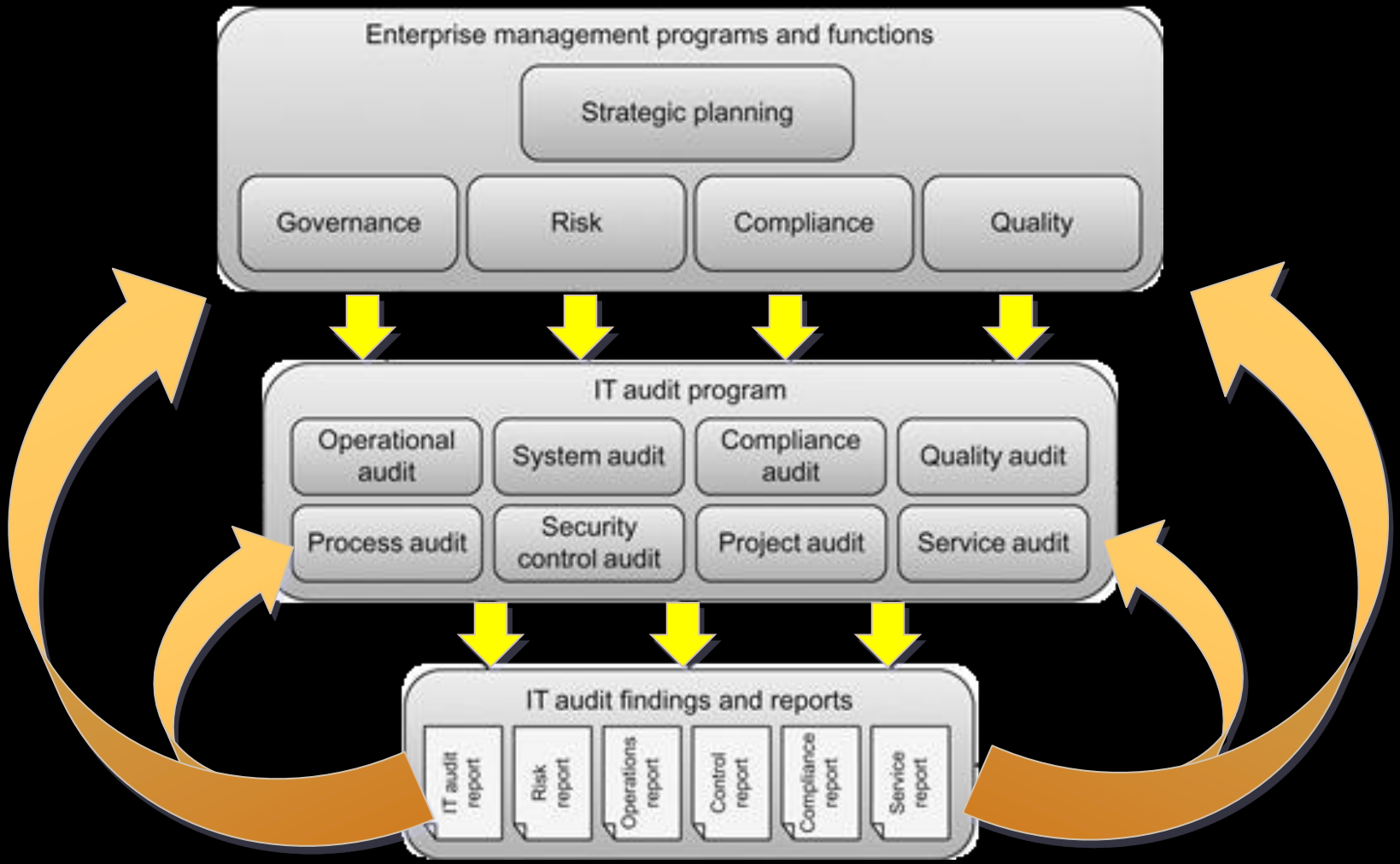
- Internal auditors : employee
- External IT Auditor:
  - consultant
  - Auditing firm
  - Certification Organization (ISACA with CISA)
  - International Organization

External Auditor from ISACA

- Certified Information System Auditor (CISA)
- Certified in Risk and Information System Control (CRISC)
- Certified Information System Manager (CISM)

How to become IT Auditor

The good thing of IT Auditing (Auditing Context)



Categories of Performance Measures

- **Performance Measurement**: What are indicators of good IT performance?
- **IT Control Profile**: How can we measure the effectiveness of our controls?
- **Risk Awareness**: What are the risks of not achieving our objectives?
- **Benchmarking**: How do we perform relative to others and standards?

IS Auditor & IT Governance

- Are IS functions aligned with organization's mission, vision, values, objectives and strategies?
- Does IS achieve performance objectives established by the business?
- Does IS comply with legal, fiduciary, environmental, privacy, security, and quality requirements?
- Are IS risks managed efficiently and effectively?
- Are IS controls effective and efficient?

Audit: Recognizing Problems

- End-user complaints
- Excessive costs or budget overruns
- Late projects
- Poor motivation - high staff turnover
- High volume of H/W or S/W defects
- Inexperienced staff – lack of training
- Unsupported or unauthorized H/W S/W purchases
- Numerous aborted or suspended development projects
- Reliance on one or two key personnel
- Poor computer response time
- Extensive exception reports, many not tracked to completion

Audit: Review Documentation

- IT Strategies, Plans, Budgets
- Security Policy Documentation
- Organization charts & Job Descriptions
- Steering Committee Reports
- System Development and Program Change Procedures
- Operations Procedures
- HR Manuals
- QA Procedures
- Contract Standards and Commitments
  - Bidding, selection, acceptance, maintenance, compliance

IT Governance

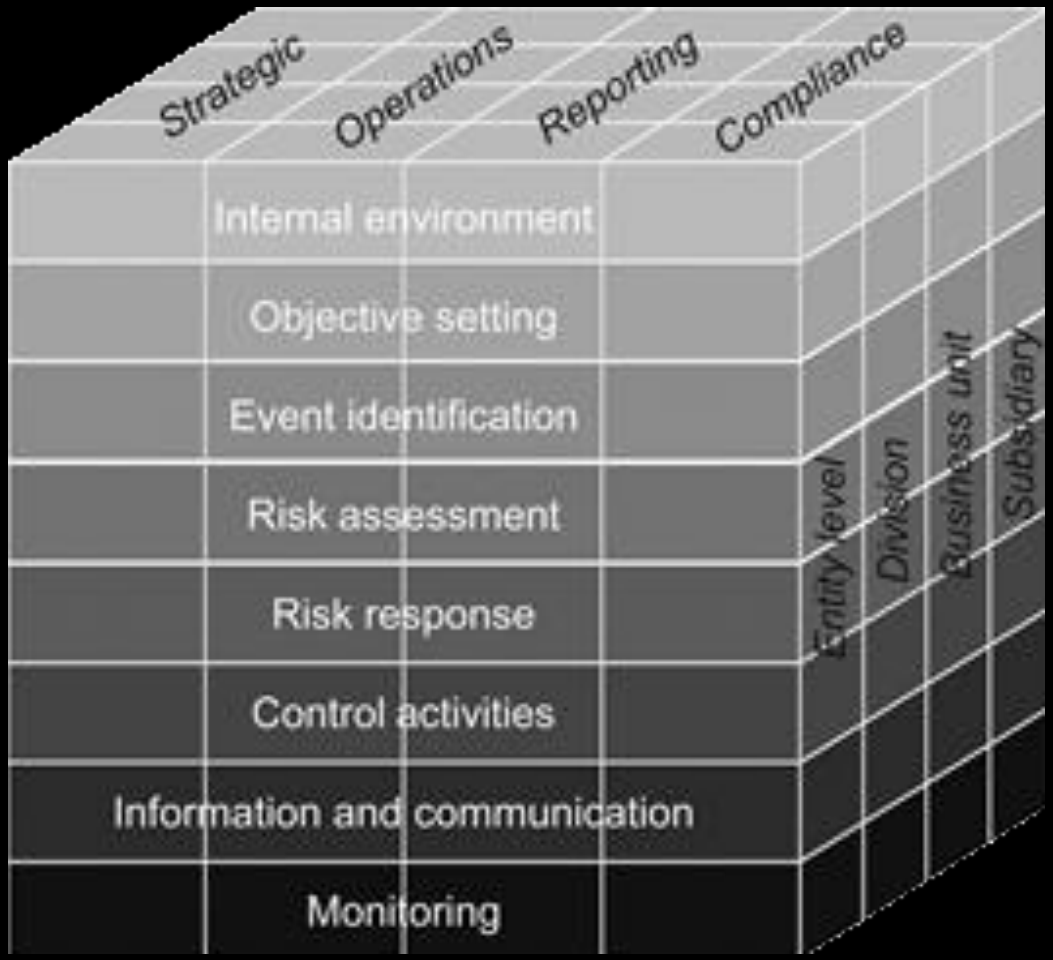
- The main idea from COBIT with five key area:

IT Governance

Also supported by

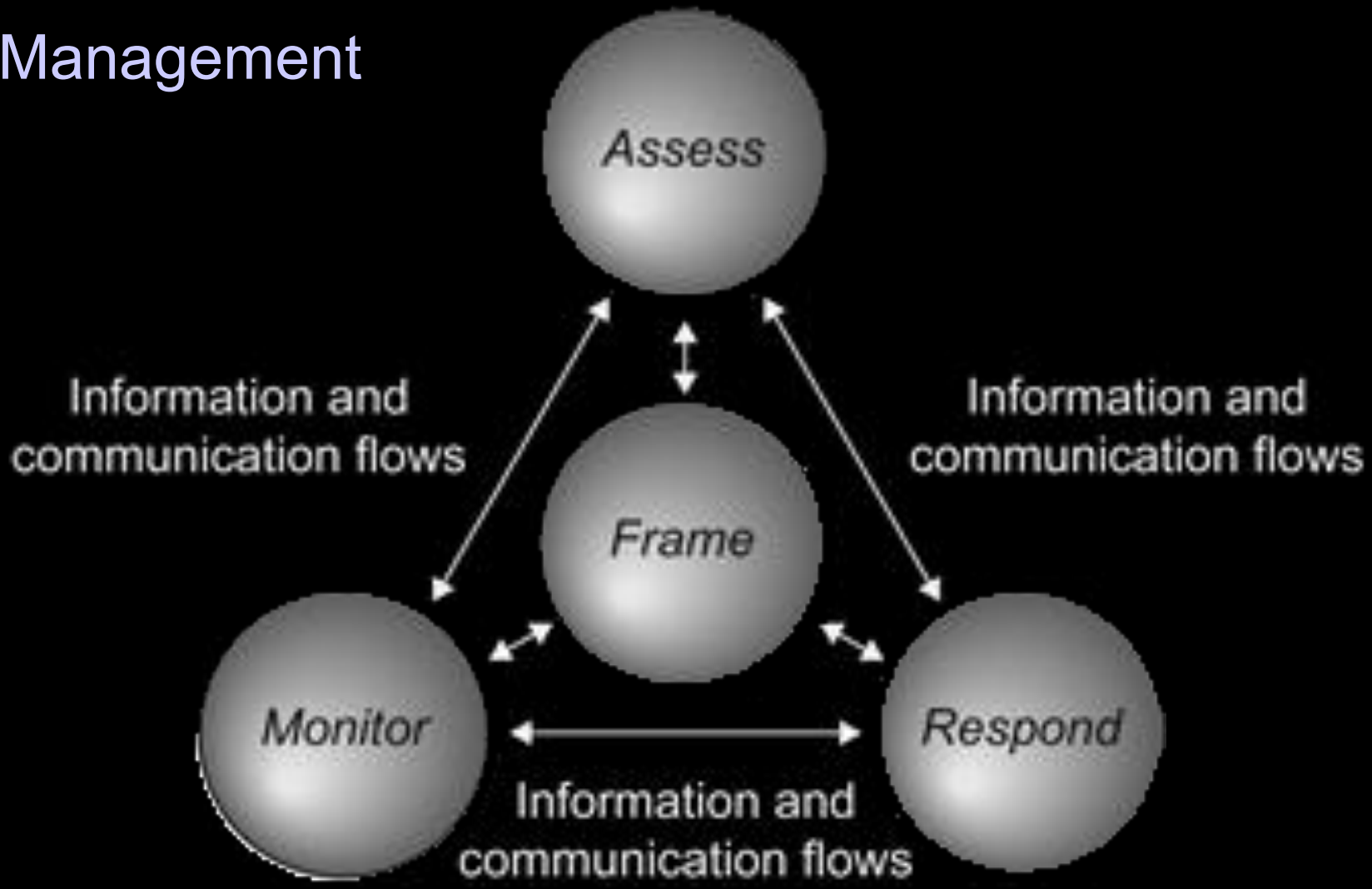
- The Information Technology Infrastructure Library (ITIL) and ISO/IEC 20000 for service management;
- The Project Management Body of Knowledge (PMBOK) and Projects in Controlled Environments version 2 (PRINCE2) for project management;
- Capability Maturity Model Integration (CMMI) and ISO/IEC 15504 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.

Risk Management



COSO's enterprise risk management framework

Risk Management



NIST's risk management framework

Compliance and certification

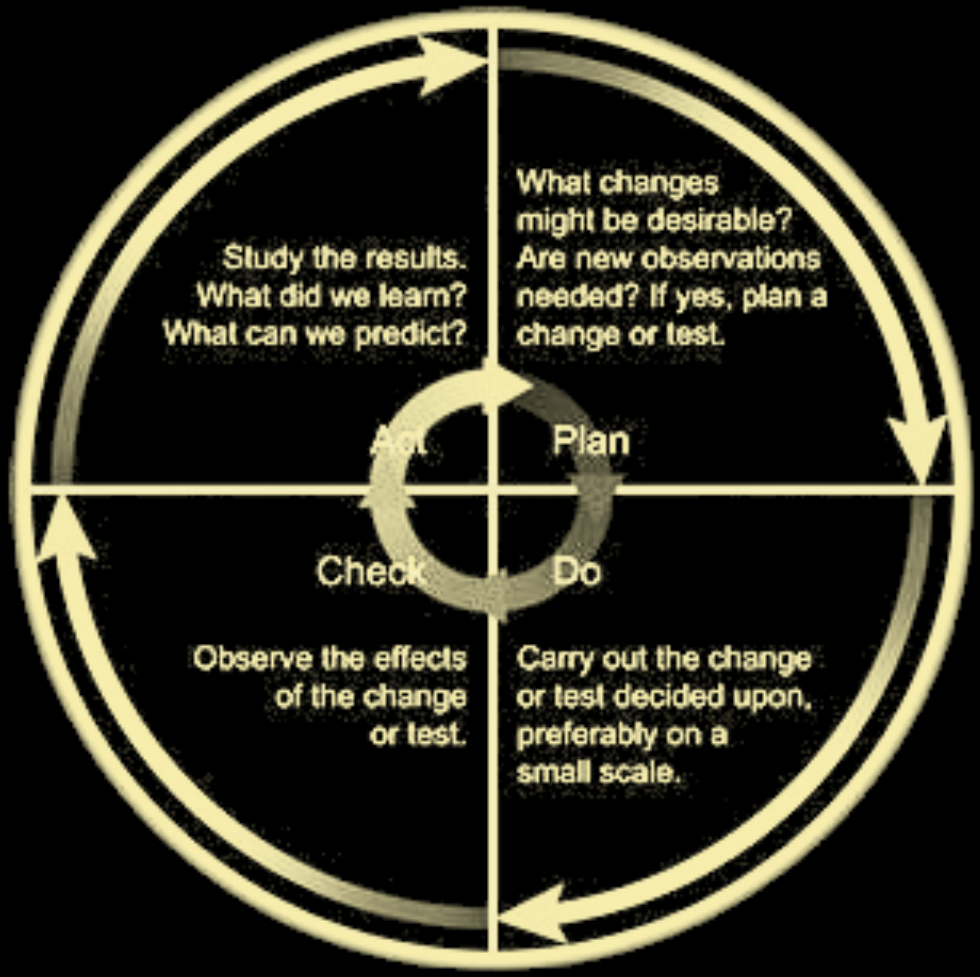
Types of Organizational Certifications and Standards

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)

Quality management and quality assurance

ISO 9001

The PDCA cycle popularized by W. Edwards Deming



Information Security Management System

The ISMS process defined in ISO/IEC 27001 applies the familiar PDCA model