UNIVERSITAS KOMPUTER INDONESIA

[TAR] Chap 14

Chapter 7: OPERATIONAL RISK MANAGEMENT

Dr. Ir. Yeffry Handoko Putra, M.T

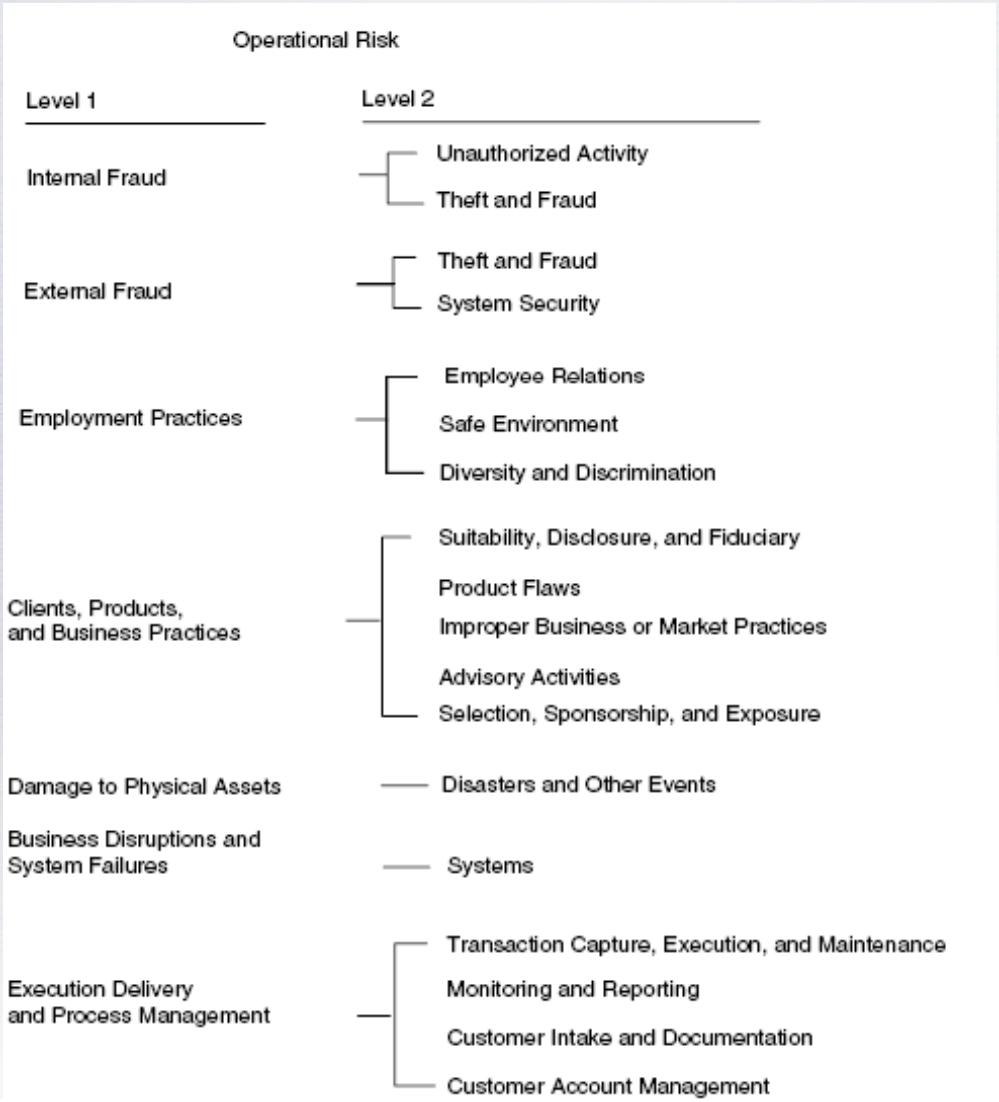
IT Governance Focus on

1. Strategic alignment
2. Value delivery
3. Risk management
4. Resource management
5. Performance management

OPERATIONAL RISK MANAGEMENT (ORM)

- Risk and opportunity go hand in hand—two sides of the same coin
- Operational risk is caused by the failure of internal controls over people, process, technology, and external events.
- Problems included : external fraud, internal fraud, inadvertent errors, technology failures, incorrect data entry, natural disasters, regulatory changes, terrorism, and so on

OPERATIONAL RISK CATEGORIZED



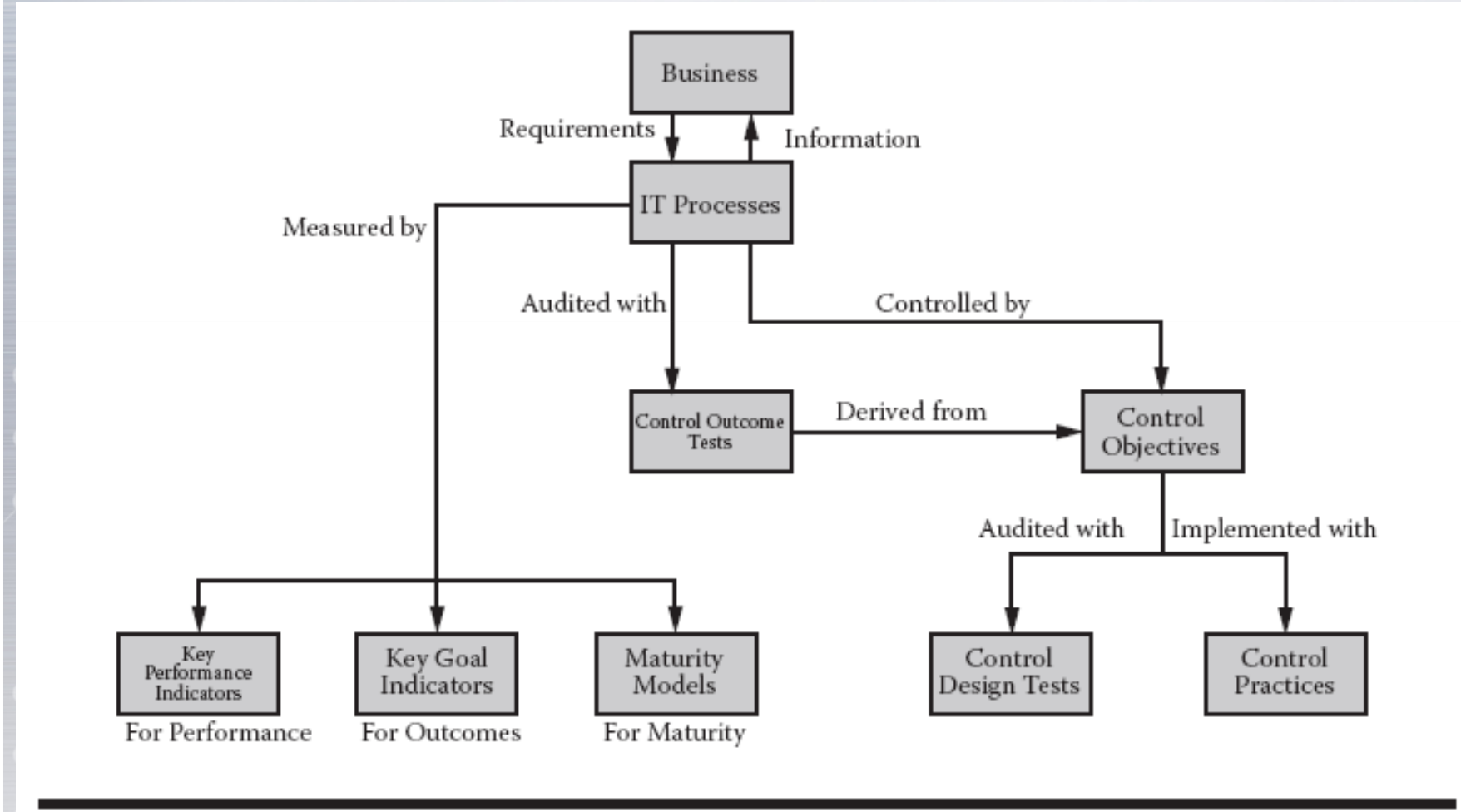
Scope of Operational Risk

- The organization has defined operational risk management on an enterprise wide level and is able to explain and defend its definition against peer organizations, regulations, and best practice frameworks.
- The organization has agreed on the boundaries to operational risk (e.g., whether it excludes or includes credit, market, legal, and reputational risk).
- The organization understands how operational risk may impact the quality and stability of earnings.

DOCUMENTATION

- Key performance indicators (KPIs)
- Key risk indicators (KRIs)
- Scorecards
- Benchmarks
- Business continuity planning
- Risk/control matrices (typically used in COSO-based regimes such as U.S. Sarbanes-Oxley, France's LSF, Germany's KonTrag, etc.)
- Stress testing and scenario analysis
- For financial institutions, a value at risk (VaR) analysis

COBIT FLOW


Business
Requirements
Information
IT Processes
Measured by
Audited with
Controlled by
Control Outcome Tests
Derived from
Control Objectives
Audited with
Implemented with
Key Performance Indicators
For Performance
Key Goal Indicators
For Outcomes
Maturity Models
For Maturity
Control Design Tests
Control Practices

POLICIES AND PROCEDURES

- The organization has in place a consistent and enterprise-wide process for the creation, collaboration, review, approval, and training/certification for these policies and procedures.
- These policies and procedures are published online and made available to employees, customers, suppliers, and regulators.

INDEPENDENT AUDIT

- The organization has regular independent reviews of all critical systems and procedures that impact operational risk.
- The independent reviews include a complete audit trail and a system of findings and recommended changes.
- The independent audit findings are reviewed on a regular basis by the risk and audit committees.

BUSINESS RESILIENCY PLANNING (BRP).

- The organization has in place business resiliency plans (BRPs) that include disaster recovery from natural and man-made disasters.
- The BRP includes time lines, resources, tasks, and costs to get the organization up and running again.
- The BRP includes an analysis of critical outsourced processes.

MANAGEMENT OVERSIGHT

- The organization has a sound management control environment that includes segregation of duties, application and database controls over transactional and master-level data, and physical and logical controls over assets and data.
- The organization has identified potential high-risk areas and implemented the appropriate enhanced monitoring and management.
- The organization enforces an active rotation and forced vacation policy. (This has been shown to prevent fraud and expose internal control failures.)

MANAGEMENT OVERSIGHT (2)

- The organization enforces strict documents and records management that requires publication, access, and version control of all sensitive information.
- The organization has controls and incentives in place to support reporting and whistle-blowing with regard to fraud and unintentional errors.
- The organization has viable programs in place to detect and investigate untoward or suspicious behavior.
- The organization exercises the same level of control over outsourced activities that impact financial reporting as it does over internal activities.

MANAGEMENT OVERSIGHT (3)

- The organization fully supports and reinforces a moral and ethical culture that includes transparency and openness, and does not tolerate the hiding of mistakes or unethical behavior.
- The ethics policy clearly describes expected business conduct standards and actions to be taken when there are lapses. The policy makes it clear that every actor is responsible for preventing and detecting fraud, corruption, or unintentional errors. This policy is shared with customers, suppliers, and the community.