FOX | ITACS
Master of IT Auditing & Cyber-Security
Fox School of Business
TEMPLE UNIVERSITY

IT Audit Process

Prof. Liang Yao

Week Three – IT Risk Assessment

Defining Risks

- Inherent Risk: The risk that an activity would pose if **no controls** or other mitigating factors were in place (the gross risk or risk before controls)

- Residual Risks: The risk that remains **after controls** are taken into account (the net risk or risk after controls).

Inherent Risks Characters

- Intrinsic to the nature of the business, activity, products or system being audited
- Will probably happen
- Internal or external
- LoB and process are all subject to inherent risk
- Inherent risk examples:
  - Nature disaster
  - Regulatory environment changes
  - Market Velocity
  - Competition
  - Introduce of new technology

Inherent Risks Assessment

- Impact
  - Industries/business sectors
  - Transaction volume
  - Transaction dollar amount
  - Regulatory environment
  - Complexity of the operational environment
  - Reputation
- Likelihood

Sample IT Risk Categories

Architecture Risk: IT structures that fail to support operations or projects.
Artificial Intelligence Risks: A special category of risk associated with technologies that learn and self improve.
Asset Management Risk: Failure to control IT assets such as loss of mobile devices.
Audit Risk: The chance that an IT audit will miss things such as security vulnerabilities or legacy risks.
Availability Risk: Downtime of IT services.
Benefit Shortfall Risk: Investments in IT that fail to achieve projected return on investment.
Budget Risk: IT programs, projects or operations teams that go over budget. In many cases, going under budget is considered a positive risk.
Capacity Risk: Capacity management failures such as an overloaded network connection that causes inefficiencies such as process failures.
Change Control: A failure to control change to complex systems including practices such as change management and configuration management.
Compliance Violations Risk: The potential that you will violate laws or regulations.

Sample IT Risk Categories (cont.)

Contract Risk: A counterparty that fails to meet its contractual obligations to you such as violations of a service level agreement.
Data Loss Risk: Loss of data that can not be restored.
Data Quality Risk: Poor quality data that causes losses due to factors such as process failures, compliance issues or declining customer satisfaction.
Decision Quality Risk: Sub-optimal decision automation or inaccurate decision support information such as analytics.
Design Debt Risk: A low quality design that results in future costs.
Facility Risk: Risks related to facilities such as data centers.
Infrastructure Risk: Failures of basic services such as networks, power and computing resources.
Innovation Risk: A special category of risk associated with experimentation and aggressive rates of change. Typically requires novel approaches to risk management such as designing activities to fail well.
Integration Risk: The potential for integration of organizations, departments, processes, technology or data to fail.

Sample IT Risk Categories (cont.)

Legacy Technology: Technology that is out of the date to the extent that it is difficult to maintain and at risk of failures.
Operational Risk: The potential for technology failures to disrupt core business processes.
Partner Risk: Risks associated with technology partners such as service providers.
Physical Security: Physical security related to IT such as security at data centers.
Process Risk: The potential for processes to be disrupted by IT failures.
Procurement Risk: Procurement is the purchasing of services, products and resources. It is prone to a number of risks including the chance of fraud, cost and quality issues.
Project Risk: In many cases, IT projects have a high rate of failure due to a number of risk factors such as scope creep, estimation errors and resistance to change.
Quality Risk: Failures of quality assurance and other quality related practices such as service management.
Regulatory Risk: The potential for new information technology related regulations.
Resource Risk: An inability to secure resources such as skilled employees.
Security Threats: Security threats such as malware and hackers.

Sample IT Risk Categories (cont.)

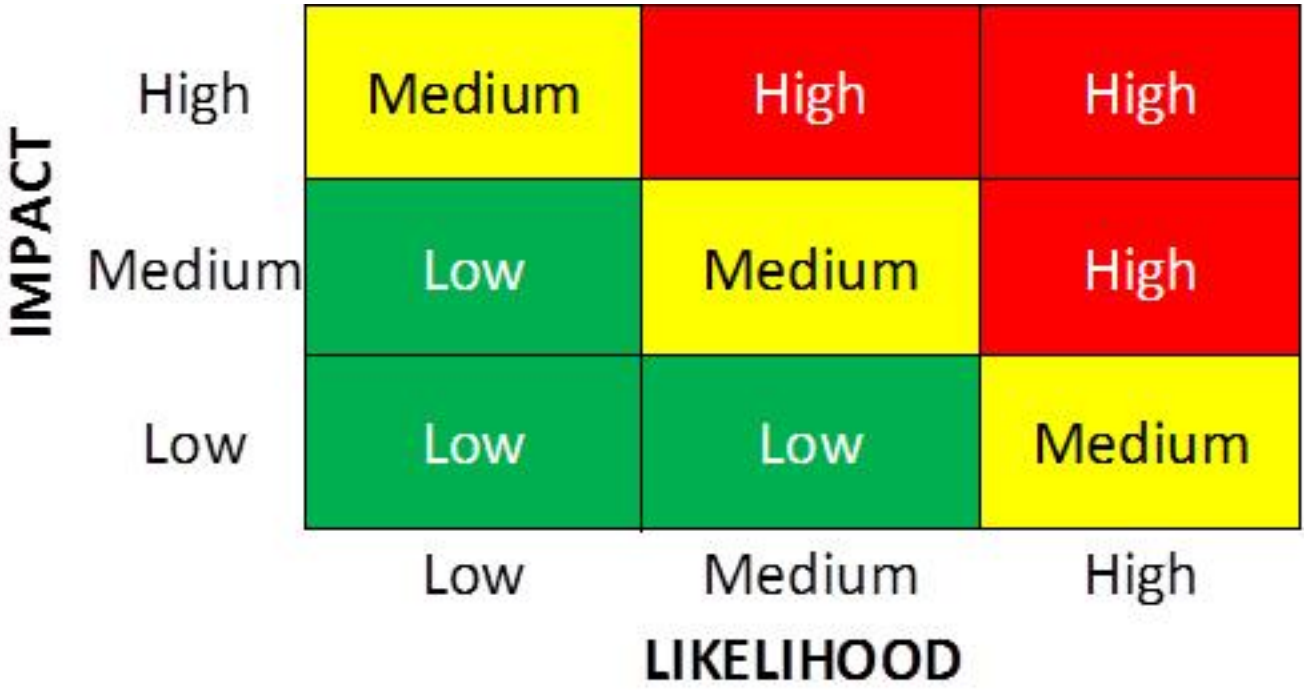
Security Vulnerabilities: Security vulnerabilities such as weak passwords and poorly designed software.
Single Point Of Failure: A small component of a large system that brings the entire system down when it fails.
Strategy Risk: The risks associated with a particular IT strategy.
Technical Debt: Weak technology implementations that are likely to result in future costs such as a big ball of mud.
Transaction Processing Risk: Failures of transaction processing such as ecommerce purchases.
Vendor Risk: The potential for an IT vendor to fail to meet their obligations to you.

Source: https://simplicable.com/new/technology-risk

Residual Risk

- After assessing the controls
- Risk mitigating/reducing vs. elimination
- Management's risk acceptance practice
- Cost vs. Benefit

Defining Risks



COSO Framework

COSO has issued the 2013 Internal Control — Integrated **Framework** (**Framework**). The **Framework** published in 1992 is recognized as the leading guidance for designing, implementing and conducting internal control and assessing its effectiveness.

Control Environment

- Commitment to employees
- Policies and procedures
- Organization Structure
- “Tone At the Top”
- Philosophy and Operating Style of Management
- Ethics and Value
- Responsibilities and Accountability

- Q: The root cause of the 2008 financial crisis

Risk Assessment

- Risk identification
- Risk analysis and assessment
  - Materiality or significance (Impact)
  - Likelihood
- Risk management
- On-going process
- Internal vs. external
- Three lines of defense concept
- Risk can be:
  - Mitigated/Reduced: e.g. robust controls
  - Accepted:
  - Transferred: cyber insurance

Control Activities

- Control definition: *"any action taken by management, the board and other parties to manage risk and increase the likelihood that establishes and goals will be achieved. Management plans, organizes and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.*
- Control types:
  - Preventive
  - Detective
  - Corrective
  - Deterrent

Source: 2013 IIA International Professional Practices Framework (IPPF)

Sample Control Activities

- Segregation of Duties
- Logical and physical access controls
- Quality review
- Participation in training
- Authorization
- Authentication
- Reconciliation
- Disaster Recovery

Information and Communication

- Information
  - Complete
  - Relevant
  - Timely
  - Concise
  - Clear
- Communication
  - East - West
  - North – South
  - Formality

Monitoring

- Performance
- Capacity
- Anomalies
- Evidence
- Accountability
- Monitoring types
  - On-going
  - Real-time
  - Ad hoc monitoring

Monitoring

- Status updates (e.g. IT projects, roadmaps)
- Trending analysis (change management, cyber threats)
- Employee opinion survey
- QA/ QC