IT Service Delivery And Support Week Five - IT Risk Assessment

IT Auditing and Cyber Security

Fall 2016

Instructor: Liang Yao

Risk Assessment Overview

Control Environment (COSO framework):

The control environment sets the tone of an organization. It influences the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

Control environment factors:

* the integrity, ethical values and competence of the people;
* management's philosophy and operating style;
* the way management assigns authority and responsibility and organizes;
* develops its people, and policies and procedures for the prevention and detection of fraud, etc.

IT Risk Assessment Steps

* Inventory of IT Operational Environment
* Identify Vulnerabilities & Controls
* Determine Residual Risk (and what to do about it?)
* Reporting

IT Risk Definition Samples

* IT Governance
* Application Development
* Documentation
* Change Control
* Security
* Desktops/Servers
* Disaster Recovery
* Data Center Operations and Physical Security
* Data Transfer and Transmission
* Data Integrity
* End-User Computing
* Telecommunication
* Vendor Reliance

IT Governance Risks

* Lack of an Effective Governance Structure
* Inadequate Staffing, Budget, and Strategy
* Improper Strategic Direction

Application/System Development Risks

* Inadequate App./System requirements review, approval and documentation
* Insufficient operational documentation
* Inaccurate scope and budget
* Un-cleared roles and responsibilities
* Inadequate testing (Dev/test/prod environment; function/UAT testing, etc.)
* Lacking security framework
* Lacking MIS reporting
* Lacking PMO function
* Not following SDLC methodology
* Developers' access to the production
* Lacking system/application documentation

Technology Documentation Risks

* No system and application documentation exist
* Incompletion of technology documentation
  * IT Policies, procedure and standards
  * Network diagram/architect
  * Server configuration/hardening, etc.
* Incorrect or inaccurate IT documentation
* Lacking of procedure documentation
  * Change management
  * Data center run-book
* Critical system and application doc. are not stored off-site
* Lacking retention policies and practices

IT Change Control Risks

* Inadequate library management standards
* Inadequate version control
* Insufficient change authorization
* Lacking process guidance: change request -> review and approval ->testing
* Inadequate access control to production environment
* Mismanaged emergency changes

Information Security Risks

* Lacking security policies and procedures
* Not conducting IT security risk assessment
* No or incomplete HW inventory
* Inadequate authentication and authorization
* Lacking security monitoring
* Inadequate assessment of third party control environment
* Inadequate security training and education
* Weak password controls
* Improperly deployed or configured firewalls and IPS/IDS

Desktop and Server Risks

* Lacking desktop and server inventory list
* Out-of-date anti-virus and malware software
* Weak Admin. access
* Lacking regular scan (to pickup unauthorized programs)
* Lacking build standards

Disaster Recovery Risks

* Inadequate DR plan
* Insufficient DR plan testing and document
* Data center specific: primary and secondary
* Missing Business Impact Analysis: RTO/RPO
* Vendor consideration
* BCP/DR files storage

Data center Operational Services and Physical Security Risks

Operational Services

* Job scheduling
* Operational activity monitoring
* SLA for key services provided
* Back up and back up status monitoring
* Environmental safeguard

Physical Security

* Physical Access
* Visitors
* Access log monitoring
* Facility Maintenance
* Background check for operational personals

Data Transition Risks

* Interfacing system (garbage-in-garbage-out)
* Monitoring
* Data encryption
* Job scheduling

Data Integrity Risks

* No validation check
* No exception review and handling
* Many manual intervention (data error…)
* Multiple data entry points (duplicate data)

End-User-Computing Risks

* EUC strategy and risk assessment
* EUC security
* Program change process
* EUC backup
* Documentation

Telecommunications

* Lacking system and security standards
* Inadequate capacity planning
* Lacking DR plan
* Inadequate control of remote access
* Lacking traffic monitoring
* Improper hardware configuration

Vendor Reliance Risks

* SLA monitoring
* Due diligence
* Contract review
* Background check for employees at the vendor side
* Access control
* Segregation of Duty from vendor side

IT Risk Rating Samples

High Risk Samples:

* Disclosure of private customer information
* Organization not to stay in compliance with Laws and Regulations
* Significant impact on the reputation of the company
* Prevent the organization from doing business for an unacceptable period of time
* Significant impact on the reputation of the company
* Sgnificant financial loss for the company

IT Risk Rating Samples

Medium Risk Samples

* Degraded service to the customers
* Delay internal operations for a short period of time
* Minimally impact reputation
* Small to medium financial loss for the company

Samples of Vulnerabilities and Threats to OS

* Domain User Accounts
* Virus
* DDoS Attack
* IP Spoofing
* Password Cracking
* Physical Access
* Back up
* Etc.…

OWASP Mobile App. Top 10 Risks

(The Open Web Application Security Project)

Identify Controls

* Authentication and Authorization
* Strong Password Requirement
* Patch Management
* Data backups
* Encryption
* Physical Security
* User Education and Training
* Etc.

Control Attributes

Control Attributes:

* Primary or secondary
* Control Types
  * Preventive
  * Detective
  * Corrective
  * Deterrent
* Manual or Automated
* Frequency of the Control Performed - > Sample
* Control Group

Control Assessment and Testing

* Step 1 – Evaluate the "Design" of the controls
  * Is there a control "Gap"?
  * Is the design of the control adequate?
  * If "N" – Discuss with management and prepare the finding; if 'Y" -> Step 2
* Step 2 – Testing the "Operating Effectiveness" of the controls

Prepare Risk & Control Metrics

* Starts with “Inherent Risks”
* Analysis the IR from Likelihood and Impact aspects
* DO NOT take any controls into consideration
* Provide Risk Rating (likelihood/impact/overall)
* Provide risk rating rationales (rationales should support the risk rating)

* Identify “controls” that can mitigate the IRs
* Assess the “design” of the controls
* Develop testing steps if “design” is adequate