Risk management

Chapter 3: It Risk and Fundamental Auditing Concepts

1. Distinguish between inherent risk and control risk. How do internal controls and detection risk fit in?

Inherent risk is associated with the unique characteristics of the business or industry of the client. Firms in declining industries are considered to have more inherent risk than firms in stable or thriving industries. (water distribution company – water can be contaminated, someone gets sick, system went down and customers cant place orders)

Control risk is the likelihood that the control structure is flawed because internal controls are either absent or inadequate to prevent or detect errors in the accounts (related to control itself, control can actually not work because of a claw or a vulnerability)

Internal controls may be present in firms with inherent risk, yet the financial statements may be materially misstated due to circumstances outside the control of the firm, such as a customer with unpaid bills on the verge of bankruptcy.

Detection risk is the risk that auditors are willing to accept that errors are not detected or prevented by the control structure. Typically, detection risk will be lower for firms with higher inherent risk and control risk.

2. Risk Categories

Controllable risks. Risks that exist within the processes of an organization and that are wholly in the hands of the organization to mitigate. (- Access to information, user name and password, access to any kind of system should be controlled)

Uncontrollable risks. Risks that can arise externally to the organization and that cannot be directly controlled or influenced but that nevertheless call for a risk position to be taken by the organization. (Earthquake)

Influenceable risks. Risks that arise externally to the organization but that can be influenced by the organization.

?Risk IT

Disaster recovery

1. For disaster recovery purposes, what criteria are used to identify an application or data as critical?

- Critical application and files are those that impact the short-run survival of the firm.
- Critical items impact cash flows, legal obligations, and customer relations.

2. Creating and Maintaining Backups

Backup software can internally designate which files have already been backed up by setting an archive bit in the properties of the file

- Differential back up will back up same file so you might have the redundant faster and you store but to process is slow.
- Incremental backup will only the one that modified, so restoring this will take time

3. Testing the Plan

Making sure the system resists the possible scenario, business continuity.

Not everything works. too expensive to protect information, so maybe buy insurance to transfer the risk to another company. Insurance might be able to deal with it. There are many types insurances.
But company could say insurance is too expensive. So what to do? self insurance.

You have to prototype; you cannot think all the risk scenario.

- Thinking the consideration of the probability
- How vulnerable
- The impact
- Short term impact, long term impact
- Which one creates what impact
- Understand
- Focus on the high risk scenario.

Testing is important

- Make fake risk scenario and test
- Make report to keep track
- Description of how to handle the disaster and update (has to update regular basis)

if the system is not available what would you do

identify system, data, network and try to prototype and based on the priority you process the plan.

your computer network affected by virus. so you network administrator, if the devices should be disconnected the network, you have the technician and see what kind of virus. if the virus is not removable and all the application and so need to be remove and reinstall. document this. so you don't need to think. follow the protocol.

ISACA Material

Enablers, IT Audit process, *Risk management, IT Risk framework*

1. What is COBIT?

The COBIT mission is to research, continually update, publicise and promote an authoritative, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals.

Risk IT Framework COBIT

IT provides a comprehensive framework for the control and governance of business-driven information-technology-based (IT-based) solutions and services
It sets good practices for the means of risk management by providing a set of controls to mitigate IT risk

1. Indicate at least 5 benefits of the IT Risk Framework.

- End to end guidance on how to manage IT related risks
- Understanding how to capitalize in IT investment made in IT internal control
- Understanding how effective IT risk management enables business process efficiency
- Promotion of risk responsibility and its acceptance throughout the enterprise
- A complete risk profile to better understand the enterprise's full exposure as a better way to utilize resources

3. Risk Management

Risk identification, assessment and evaluation is concerned with correctly determining the risk faced by the enterprise and providing recommendations to senior management on how to effectively maintain risk at an acceptable level, including, but not limited to:

Identifying risk, including emerging risk and risk associated with people, processes, technology, architecture, applications, information, natural factors and physical threats

Assessing the risk levels associated with each threat, including anticipated risk likelihood and impact and the effectiveness of current and planned controls

Calculating the risk levels using both quantitative and qualitative metrics and determining the impact of the risk on the ability of the business to meet its goals and objectives

4. Enablers

COBIT 5 for Risk provides specific guidance related to all enablers for the effective management of risk:

- The core risk management process(es) used to implement effective and efficient risk management for the enterprise to support stakeholder value
- Risk scenarios, i.e., the key information item needed to identify, analyze and respond to risk; risk scenarios are the concrete, tangible and assessable representation of risk
- How COBIT 5 enablers can be used to respond to unacceptable risk scenarios

5. Contrast the Private Encryption Standard approach with the Public Key Encryption approach to controlling access to telecommunication messages.

In the Private Encryption Standard approach, both the sender and the receiver use the same key to encode and decode the message. In the Public Key Encryption approach all senders receive a copy of the key used to send messages; the receiver is the only one with access to the key to decode the message.

Chapter 10: Audit Reporting Follow-up

1. Audit Reporting Follow-up
   - AUDIT REPORTING: Auditors communicate the overall findings together with recommendations for actions to be taken using the audit report (ex you can get together after 5pm to have meeting before going further)
   - INTERIM REPORTING: Reports prepared and issued while the audit is in progress
   - CLOSING CONFERENCES: This permits an overall review of the audit objectives and findings and is the final opportunity to clear up any misunderstandings or omissions prior to report issuance.

Chapter 26 - Information Assets Security Management

1. What are the key objectives of information security:

Confidentiality—Preserving authorized restrictions on access and disclosure, including means for protecting privacyand proprietary information

Integrity—Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity

Availability—Ensuring timely and reliable access to and use of information 5. 5

Chapter 28: Applied Information Technology Security

1. Hardening the Operating Environment (1)

Where high-value information assets are at risk or where there is a high degree of unrestricted access, attention should be paid to the degree of insecurities commonly found in standard operating environments.

- Removing unneeded functionality and Services
- Activating selected security capabilities
- Ensuring service packs and software patches are appropriately activated
- Renaming or disabling default system accounts and passwords
- Access granted on a need-to-have or least privilege basis

default system accounts..unit system.. admin account.. potential proble. ..
unnecessary access should not be created. if not i can create harm.
anti virus should be up to date coz virus keeps changes.
log files keeep all the activity.