SUNWAY

INT'L BUSINESS SCHOOL

Programme Name: **BCS HONS**

Course Code: **CSC 2734**

Course Name: **Information System Security**

Open Book Examination

Date of Submission: **5/30/2021**

Submitted By:

Student Name**: Dipesh Tha Shrestha**

IUKL ID: **041902900028**

Semester**: Third Semester**

Intake**: September 2019**

Submitted To:

Faculty Name**: Manoj Gautam**

Department**: LMS**

1. **Elaborate Information Security Risk in context to financial organization. To keep up with the competition, organization must design and create a safe environment in which business processes and procedure can function. To meet these objectives the principle of risk management are applied. Purpose FOUR (4) risk controlling strategies that any organization can choose to control risks**

Answer:

Risk management is the process of making and carrying out decisions that will minimize the adverse effects of risk on an organization. The adverse effects of risk can be objective or quantifiable like insurance premiums and claims costs, or subjective and difficult to quantify such as damage to reputation or decreased productivity. By focusing attention on risk and committing the necessary resources to control and mitigate risk, a business will protect itself from uncertainty, reduce costs, and increase the likelihood of business continuity and success.

Any FOUR (4) risk controlling strategies that any organization can choose to control risks are:

- **Avoid the Risk**

Sometimes a risk is so serious that you just want to avoid it entirely, such as by avoiding the activity or taking a completely different approach. If a particular type of trading is extremely risky, you may decide that the potential reward isn't worth the risk and abandon it.
This strategy has the advantage of being the most effective way of dealing with a risk. You eliminate the risk of losing money by stopping the activity that is causing the potential problems. However, you will lose any benefits you may have received. Risky activities can pay off handsomely or provide other benefits to your company. As a result, this strategy should only be used as a last resort after you've exhausted all other options and discovered that the risk level remains too high.

- **Reduce the Risk**

If you don't want to give up the activity entirely, one common strategy is to reduce the risk involved. Take steps to reduce the possibility of a negative outcome or to reduce the impact if one does occur. This is the most common strategy, and it can be used to manage a wide range of risks. It allows you to continue doing what you're doing, but with safeguards in place to make it less dangerous. You get the best of both worlds if you do it right. However, the risk is that your controls are ineffective, and you still suffer the loss you anticipated.

- **Transfer of Risk**

We're all familiar with the concept of insurance from our everyday lives, and the same applies in business. An insurance contract is basically a transfer of risk from one party to another, with a payment in return. When you own a home, for example, there's a big risk of losses from fire, theft, and other damage. So you can buy a home insurance policy, and transfer that risk to the insurance company. If anything goes wrong, it's the insurance company that bears the loss, and in return for that peace of mind, you pay a premium. When you own a business, you have the option to transfer many of your risks to an insurance company as well. You can insure your properties and vehicles, and also take out various types of liability insurance to protect yourself from lawsuits. We'll look at insurance in more detail in the next tutorial in the series, but it's a good option for dealing with risks that have a large potential impact, as long as you can find an affordable policy.

- **Accept the Risk**

Risk acceptance means you don't try to avoid or mitigate a risk, but instead choose to live with the consequences. This strategy is the best choice if the impact of the risk is small, and avoidance or mitigation would be more expensive than justified by the size of the impact. The last, but certainly not least, option is to just accept the risk as-is and do nothing. This risk response strategy is often used for risks with a low probability of occurring or that would have a low impact if they did happen. Many companies will have budget reserves set aside to deal with situations like this.

The advantage of accepting a risk is pretty clear: there's no cost, and it frees up resources to focus on more serious risks. The downside is also pretty clear: you have no controls in place. If the impact and likelihood are minor, that may be fine. But make sure you've assessed those things correctly, so that you don't get a nasty surprise.

2. **From the information security perspective, the termination of employee is laden with potential security pitfalls. Elaborate your idea on information security in employee termination.**

Answer:

As we know, Employee termination refers to the end of an employee's work with a company. An employee may be terminated from a job of their own free will or following a decision made by the employer. Some causes of employee termination are Low performance, Violation of Company Rules, Employee Disciplinary Action, Harassment of any sort, be it sexual, physical, mental, or emotional, Lack of cooperation and progressive discipline or Leaking information to competition etc. The employee termination process should focus on severing all ties between the employee and the company. This includes blocking the employee's internal access to all company data. Information Security should immediately revoke the former employee's computer, network, and data access. Remote access should also be removed, and the former employee should be dispossessed of all company-owned property, including technological resources such a notebook computer and intellectual property such as corporate files containing customer, sales, and marketing information. Just as the granting of access and security clearances should be documented for future reference, the revocation of access should also be documented, especially for legal purposes. The goal, of course, should always be to revoke access in ways that make good business sense financially, technologically, and legally.

The importance of information security in employee termination are given below:

Change any shared account passwords that were known by the employee

While typically discouraged, it is often a requirement that multiple users share the password to a single account. For example, the password to a local Administrator account or an application’s super-user account may be shared by more than one employee. If the employee is in possession of one of these shared passwords, it should be immediately changed.

Retrieve computing hardware from the employee
Upon separation, all computing hardware issued to an employee will need to be collected. This includes but is not limited to any University-issued laptops, desktops, computing peripherals, cell phones and hardware tokens. Any hardware token the employee may have should be immediately returned to the appropriate administrator. All other hardware can be re-used as deemed appropriate by the manager of the employee.

Change and disable application-level passwords and accounts.
Start with the business-critical applications first, such as CRMs and Financial applications. Don't forget other commonly overlooked applications such as Dropbox, which can be configured to sync data to a personal home machine.

Preemptive Preservation of Data
Every company needs to have data redundancy and retention policies that satisfy its business needs and adhere to applicable laws. Such policies address the backup, restoration, and preservation of corporate data in general. However, a company should also enact policies that detail when and how IT should go about preserving potentially and particularly sensitive data, records, logs, and other material that could be of legal significance, should the company and former employee wage a legal battle. This is especially important in the case of a former employee who held a high-level position or left the company under a cloud of suspicion.

3. **Identifying risk and managing risk is one of the key responsibilities of every manager within organization.**

a. **Explain Risk Identification process**

Risk identification is the process of determining risks that could potentially prevent the program, enterprise, or investment from achieving its objectives. It includes documenting and communicating the concern. Risk identification is the process of identifying and assessing threats to an organization, its operations, and its workforce. For example, risk identification may include assessing IT security threats such as malware and ransomware, accidents, natural disasters, and other potentially harmful events that could disrupt business operations. Companies that develop robust risk management plans are likely to find they’re able to minimize the impact of threats, when and if they should occur.

There are multiple types of risk assessments, including program risk assessments, risk assessments to support an investment decision, analysis of alternatives, and assessments of operational or cost uncertainty. Risk identification needs to match the type of assessment required to support risk-informed decision making. For an acquisition program, the first step is to identify the program goals and objectives, thus fostering a common understanding across the team of what is needed for program success. This gives context and bounds the scope by which risks are identified and assessed.

An effective risk identification process should include the following steps:

- Creating a systematic process: The risk identification process should begin with project objectives and success factors.
- Gathering information from various sources: Reliable and high-quality information is essential for effective risk management.
- Applying risk identification tools and techniques: The choice of the best suitable techniques will depend on the types of risks and activities, as well as organizational maturity.
- Documenting the risks: Identified risks should be documented in a risk register and a risk breakdown structure, along with their causes and consequences.
- Documenting the risk identification process: To improve and ease the risk identification process for future projects, the approach, participants, and scope of the process should be recorded.
- Assessing the process' effectiveness: To improve it for future use, the effectiveness of the chosen process should be critically assessed after the project is completed.

b. Propose FOUR (4) risk control strategy.

Answer:

<u>FOUR (4) risk control strategy are given below:</u>

- **Avoid**

Avoidance eliminates the risk by removing the cause. It may lead to not doing the activity or doing the activity in a different way. The project manager may also change or isolate the objective that is in trouble. Some risks can be avoided by an early collection of information, by improving communication between stakeholders or by use of expertise.

Example of this approach includes extending the schedule or changing the scope of the project activity. Another example could be a risk which is too hazardous that it may lead to loss of life and is avoided by shutting down the project altogether.

- **Transfer**

In Risk Transfer approach, the risk is shifted to a third party. The third-party, like insurance company or vendor, is paid to accept or handle the risk on your behalf and hence the ownership, as well as impact of the risk, is borne by that third party. This payment is called a risk premium. Contracts are signed to transfer the liability of risks to the third party.

Risk Transfer does not eliminate the risk, but it reduces the direct impact of the risk on the project. Few Transference tools are an insurance policy, performance bonds, warranties, guarantees, etc. This approach is most effective in covering financial risk exposure.

- **Mitigate**

Mitigation reduces the probability of occurrence of a risk or minimizes the impact of the risk within acceptable limits. This approach is based on the fundamental principle that earlier the action taken to reduce the probability or impact of a risk is more effective than doing fixes to repair the damages after the risk occurs.
Example of mitigating a risk includes the use of advanced technology or best practices to produce more defect-free products. Mitigation may require a prototype development to measure the risk level. In the case where it is not possible to reduce the probability of the risk, the risk impact reduction is targeted by identifying the linkages that determine the risk severity.

- **Accept**

Acceptance means accepting the risk, especially when no other suitable strategy is available to eliminate the risk. Acceptance can be passive acceptance or active acceptance.
Passive acceptance requires no other action except to document the risk and leaving the team to deal with the risks as they occur. In an active acceptance approach, a contingency reserve is designed to recover the losses of time, money, or resources.

c. How OCTAVE approach is used to manage Risk.

Answer:
OCTAVE is a risk based strategic assessment and planning technique for security. OCTAVE is self-directed, meaning that people from an organization assume responsibility for setting the organization’s security strategy. The technique leverages people’s knowledge of their organization’s security-related practices and processes to capture the current state of security practice within the organization. Risks to the most critical assets are used to prioritize areas of improvement and set the security strategy for the organization. OCTAVE is targeted at organizational risk and focused on strategic, practice-related issues. It is a flexible evaluation that can be tailored for most organizations. When applying OCTAVE, a small team of people from the operational (or business) units and the information technology (IT) department work together to address the security needs of the organization, balancing the three key aspects.

The OCTAVE approach is driven by two of the aspects: operational risk and security practices. Technology is examined only in relation to security practices, enabling an organization to refine the view of its current security practices. By using the OCTAVE approach, an organization makes information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information-related assets. All aspects of risk (assets, threats, vulnerabilities, and organizational impact) are factored into decision making, enabling an organization to match a practice-based protection strategy to its security risk. OCTAVE is an asset-driven evaluation approach. Analysis teams identify information-related assets (e.g., information and systems) that are important to the organization and focus risk analysis activities on those assets judged to be most critical to the organization. **Therefore, this is how OCTAVE approach is used in Risk Management.**

4. **Confidentiality of information ensures that only those with sufficient privileges may access certain information. To protect the confidentiality of information, propose at least FOUR (4) measures.**

Answer:

<u>FOUR (4) measures to protect the confidentiality of information are given below:</u>

- **Data Minimization**

One approach to data protection in a statistical environment is to minimize or eliminate the collection of personally identifiable information that is, information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

- **Restricted Data**

Restricting data includes removing explicit identifiers and applying a variety of statistical disclosure limitation methods to the dataset to reduce the risk of disclosure. To restrict data, before releasing microdata files statistical agencies remove all obvious identifiers. This approach is not sufficient, however, because some people or entities have characteristics or combinations of characteristics that are rare or unique and make them identifiable. Consequently, there are a variety of statistical disclosure limitation techniques that federal statistical agencies use to reduce the disclosure risk of microdata files.

- **Licensing**

Another way to restrict access is through licensing agreements, which provide more flexibility than online data analysis systems. Licensing agreements allow researchers access to restricted data from their home institution through the use of strict security procedures and legally binding agreements.

- **Control Access**

For any information that's stored digitally it's incredibly important that you control access to it by using passwords, firewalls and encryption. This is especially important when the information is contained on smaller storage devices such as USB drives that are easily misplaced. When using passwords to control access to confidential information, you must ensure that they're both secure and changed regularly. Using easy-to-guess passwords is a mistake that many businesses make and something that you should avoid doing if you want to keep your confidential information secure. The best type of passwords to use are a combination of upper and lower case letters and as well as special characters.

5. **Access control is a method by which systems determine whether and how to admit a user into trusted area of the organization. Purpose at least FOUR (4) access control architecture model to implement access control mechanism in an organization.**

Answer:

<u>FOUR access control architecture model to implement access control mechanism in an organization are given below:</u>

- **Mandatory access control**

Mandatory access control is widely regarded as the most restrictive model of access control available. Only the system's owner has the ability to control and manage access based on the settings defined by the system's programmed parameters. Such parameters cannot be changed or overridden. None of the permissions or privileges are under the control of the end user. They can only use the points that the system's owners have given them permission to use. MAC is typically used for facilities or organizations that require maximum security, such as government facilities, due to its high level of restriction.

- **Role-based access control**

Role-based access control, also known as nondiscretionary access control, grants access based on an individual's position within an organization. Predefined roles are linked to specific permissions in these systems. They enable the administrator to grant an individual only the level of access necessary to perform their duties. This type of access control is one of the most popular in businesses due to its simplicity. RBAC, on the other hand, has some disadvantages. When an exception to the standardized permissions is required, RBAC cannot grant one-time permissions.

- **Discretionary access control**

Discretionary access control is the least restrictive type of access control. Under this system, individuals are granted complete control over any objects they own and any programs associated with such objects. The individuals can then determine who has access to their objects by programming security level settings for other users.

- **Rule-based access control**

Rule-based access control is the last of the four main types of access control for businesses. This system grants or denies access to users based on the owner's or system administrator's dynamic rules and limitations. Access may be restricted based on a variety of factors, including the individual's location, the time of day, or the device being used. RBAC is an ideal form of access control for businesses that require a dynamic security solution because it allows you to customize rules and permissions.

<u>Thank you</u>