Programme Name: **BCS HONS**

Course Code: **CSC 2734**

Course Name: **Information System Security**

Internal Examination

Date of Submission: **4/30/2021**

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. **The overall planning for unexpected events is contingency planning (CP), Explain THREE (3) Components of Contingency planning with action plan**

Answer: As we know, Contingency planning is a strategy for assisting an organization in responding to an event that may or may not occur. Contingency plans are also known as "Plan B" plans because they can be used as a backup plan if things don't go as planned.

The three components of contingency planning are:

- **Incidence response plan (IRP)**

An incident response plan is a set of instructions designed to assist IT personnel in detecting, responding to, and recovering from network security incidents. These plans address threats to daily operations such as cybercrime, data loss, and service outages. Incident response plans provide instructions for responding to many potential scenarios, including data breaches, denial of service/distributed denial of service attacks, firewall breaches, virus or malware outbreaks or insider threats. Without an incident response plan in place, organizations may either not detect the attack in the first place, or not follow proper protocol to contain the threat and recover from it when a breach is detected.

- **Disaster recovery plan (DRP)**

An organization's disaster recovery (DR) plan is a formal document that contains detailed instructions on how to respond to unplanned events such as natural disasters, power outages, cyber-attacks, and other disruptive events. The plan includes strategies for minimizing the effects of a disaster so that a company can continue to operate – or quickly resume critical operations. A disaster recovery plan should address both intentional and unintentional man-made disasters, such as the fallout from terrorism or hacking, as well as unintentional disasters, such as equipment failure.

- **Business continuity plan (BCP)**

A business continuity plan (BCP) is a document that outlines how a company will keep running in the event of an unplanned service interruption. It's more comprehensive than a disaster recovery plan, as it includes contingencies for business processes, assets, human resources, and business partners – all aspects of the company that could be impacted.

2. **Explain Bull eyes model for policy Centre decision making.**

Answer: Bull's eye model is the information security program that focuses on role of policy. A bull's eye model is a strategic template designed in the shape of a bull's eye. It helps teams work out where their real priorities lie. Each concentric circle radiating out from the center corresponds to a different level of importance. The inner-circle should hold only the absolute top-priority tasks, all the way to the outermost circle which holds the least important tasks.
Any organization's strategic planning is essential. You can make a dynamic business strategy presentation using these bull's eye model templates. An organization's primary task is to establish goals and objectives. It necessitates a thorough examination of the subject. To achieve your objectives, you must devise strategies and plans. But the story doesn't end there. It will take a team effort to reach the goal. Your team must be well-versed in the company's strategies and stages. You can creatively acknowledge your audience about the goals and ways to achieve them with the bullseye model. Therefore, Bull eyes model is important for policy Centre decision making.

3. **Explain the concept of EISP with example**.

Answer: The enterprise information security policy (EISP), also known as a general security policy or IT security policy, is, generally, a document, or regulation, that governs company information security policy. The company's security efforts are topped by an Enterprise Information Security Policy. In fact, it explains a company's security philosophy and assists in determining the direction, scope, and tone of an organization's security efforts. It's a management-level document, which means it was probably written by the company's chief information officer or someone in a similar position. The EISP, or Enterprise Information Security Plan, explains what the company believes about security, the various types of roles that exist in the company's security arena (along with their responsibilities), and the responsibilities that all employees have for keeping the organization's systems and information safe from intrusion.

An EISP will vary from one company to another to meet the purpose of the organization itself. For example, a University that handles a lot of student and teacher data in electronic form may specify as one of its EISP goals to safeguard against authorized access or accidental dissemination. In this way, it is possible to integrate the mission and objectives of the organization into its EISP by defining

specific security measures that can enhance and further the organization's purpose.

4. **Describe Ten Commandments of InfoSec Awareness Training.**

Answer: InfoSec Awareness Training or Security awareness training is the process of providing formal cybersecurity education to your workforce about a variety of information security threats and your company's policies and procedures for addressing them. Topics covered in security awareness training often expand beyond the digital world and discuss physical security and how employees can keep themselves and loved ones secure. Such training can take a variety of forms but is most often presented in an online or computer-based format.

Ten Commandments of InfoSec Awareness Training are:

1. Information security is a people, rather than a technical, issue.
2. If you want them to understand, speak their language.
3. If they cannot see it, they will not learn it.
4. Make your point so that you can identify it and so can they.
5. Never lose your sense of humor.
6. Make your point, support it, and conclude it.
7. Always let the recipients know how the behavior that you request will affect them.
8. Ride the tame horses.
9. Formalize your training methodology.
10. Always be timely, even if it means slipping schedules to include urgent information.

- **Information security is a people, rather than a technical, issue.**

All technical tools, such as access control software, firewalls, hardware identifiers, and other hardware/software controls, are aimed at limiting human access to system assets. As a result, the cooperation of those who use such tools must be sought. This concept is built on the foundation of baseline policies, standards, and procedures. It means that people are the one who protect the information.

- **If you want them to understand, speak their language.**

People from different backgrounds and work environments might not be familiar with the of the information technology (IT) field. So people should learn to speak their language and communicate with them in it. Communication is important so it mean that all the people must have a common language for example like English.

- **If they cannot see it, they will not learn it**.

It means that if the person cannot see the step or the process of the works, they cannot do that or cannot understand that.

- **Make your point so that you can identify it and so can they.**

At least one point must be communicated in every communication. Make sure it's easy to find and understand, as well as what it's for. The reason for the communication, as well as the actions requested and their justifications, should be included in each point. It means make your point short and clear so everyone can understand it easily.

- **Never lose your sense of humor.**

No matter how serious a problem is, it can be addressed without resorting to biblical references. There are times when it is appropriate to make light of the situation; learn to do so and apply a sense of humor to them. This isn't to say that your communication should be funny, but it shouldn't be so dry that it turns off readers. It means the staff should not lose their humor while doing their job.

- **Make your point, support it, and conclude it.**

Do not bury people in buzzwords. The second page of a report or a press release is rarely read. The presence of a third or more pages reduces the likelihood of any of it being read carefully, and this decrease is inversely proportional to the number of pages presented. Its mean to make your point or statement short, clear and meaningful

- **Always let the recipients know how the behavior that you request will affect them.**

People want to know how much something will cost them if they take a specific action. Their understanding of the need for security could be demonstrated by

stating how the organization's profitability is directly proportional to their position and income.

- **Ride the tame horses.**

Every business has communication media in place, as well as personnel to maintain and distribute them. They are usually on the lookout for good copy and can help you get your message across. Make use of their abilities and the vehicles that are already in place. It means to use the ability of every employee properly in right place and in right time

- **Formalize your training methodology.**

Build a program that includes both written and oral communication, as well as brief but formal classwork. Keep track of who has attended the class and when they did so. Set up a for-profit "security agreement" that must be renewed every year. Maintain a reasonable and minimal number of such communications within a given timeframe when using printed or electronically distributed media. Its mean there should be a proper way to teach the ethics and other.

- **Always be timely, even if it means slipping schedules to include urgent information**.

It means that all the staff should be ready to work in case of denial of service/distributed denial of service attacks, firewall breaches, virus or malware outbreaks or insider threats.