**CIE-5 –2024**

**CYBER SECURITY 20CS54IT**

**Scheme of Valuation**

|  |  |  |
| --- | --- | --- |
| **Q.NO** | **Description of Questions** | **Marks**  **Allotment** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**1.a) What is incident management? Explain stages and life cycle of incident management life cycle? List the best practices of incident management.**

Incident management is the process of detecting, investigating, and responding to incidents in as little time as possible. While it doesn’t always lead to a permanent solution, incident management is important in order to finish projects on time, or as close to the set deadline as possible.

There are five steps in an incident management plan:

1. Incident identification
2. Incident categorization
3. Incident prioritization
4. Incident response
5. Incident closure

1. Incident identification

The first step in an incident response plan is identifying the incident. An issue can arise in almost any part of a project, whether that’s internal, vendor-related, or customer-facing.

To identify an incident, you should include the following:

* Name or ID number
* Description
* Date
* Incident manager

### 2. Incident categorization

Incidents need to be accurately categorized in order to be correctly resolved. Categorization allows your team members to:

1. Quickly find a solution if this incident ever arises again.
2. Correctly prioritize incidents and sort them by urgency.

### 3. Incident prioritization

Once an incident is identified and categorized, you can move on to incident prioritization. There are a couple of key things to consider when it comes to ranking project incidents by importance:

* Which other incidents you’re prioritizing against
* What other tasks need to be completed

### 4. Incident response

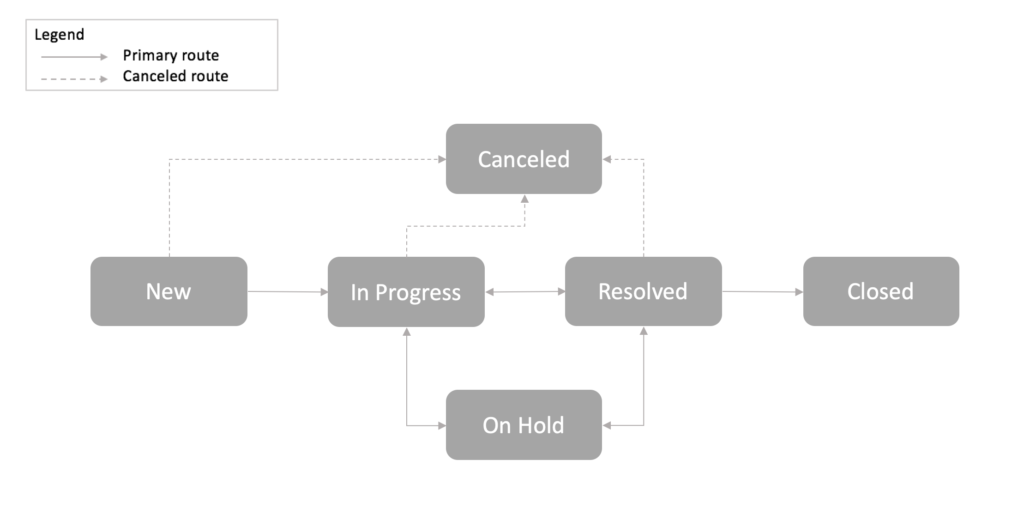
Once the incident is correctly labeled and prioritized, you can dig into the meat of the issue. Depending on how it’s labeled, the incident should be sent to the team most equipped to troubleshoot. Usually, the appropriate team will be able to quickly handle the problem. Quick response times are key to incident management.

### 5. Incident resolution and closure

Once the problem is solved to everyone’s satisfaction, you’re ready to close the ticket and log the incident as complete. You’ll want to keep any documentation you’ve created in the above steps by storing it in a shared workspace for future reference. This can be anything from a shared drive to a digital project folder.

**Incident Management Life cycle**

**Incident management State Model Flow**



|  |  |
| --- | --- |
| **State** | **When Used** |
| New | Initial state of any new incident |
| In Progress | Set automatically upon assignment to an individual |
| On Hold | Investigation paused while awaiting information from the customer or an external vendor, or for provision of information, evidence, or a resolution from a related problem or change |
| Resolved | Service restored; awaiting customer confirmation or automatic closure |
| Closed | Final state of the incident, following automatic or manual closure |
| Canceled | Incident raised in error or identified as a duplicate of another incident record |

Incident management best practices.

### 1. Identify early and often

### 2. Keep your work tidy

### 3. Educate your team

### 4. Automate tasks

### 5. Communicate in one place

### 6. Use project management tools

### 7. Continue improving

**OR**

**2.a) Explain GRC in a company with its benefits and its Importance?**

GRC stands for Governance, Risk Management, and Compliance. It refers to a set of processes and

technologies used by organizations to manage and monitor compliance with legal and regulatory requirements, manage risks and ensure that the company is operating in an ethical and transparent manner.

The benefits of a strong GRC program in a company include:

1.Improved Risk Management: By having a clear understanding of the risks facing the company and

implementing strategies to manage those risks, companies can minimize potential harm and maximize

opportunities.

2.Increased Compliance: GRC helps ensure that the company is following all relevant laws, regulations,

and ethical standards, reducing the risk of fines, legal action and reputational damage.

3.Enhanced Transparency: A strong GRC program promotes transparency in the company's operations

and decision-making processes, which can increase trust among stakeholders and enhance the

company's reputation.

4.Efficient Use of Resources: By streamlining processes and utilizing technology to automate GRC

activities, companies can reduce the time and cost associated with managing risks and ensuring

compliance.

5.Improved Decision Making: By having a comprehensive understanding of the company's risks and

compliance obligations, companies can make better-informed decisions that promote long-term success.

**Section-2 (Practical) - 20 marks**

**3a) Using VIRUSTOTAL website Analyze any File, URL & Domain etc.**

Step 1: - Go to any browser and search <https://www.virustotal.com>

Step 2: -Click choose file to scan a file

Step 3: - Select any file and click open

Step 4: -Now select URL option and enter any URL and click enter to start a scan

Step 5: -Now select search and enter URL, Domain, IP address and press enter

**3b) Install the APK tool on your virtual machine and perform reverse engineering of any application.**

Open terminal in kali Linux

Step 2: - Install apktool using this command “sudo apt install apktool” & press Enter button. If installation not begin / any error show update “sudo apt update”

Step 3: - Wait until installation complete

Step 4: - Download Diva application using “git clone <https://github.com/xAltmime/diva-apk-file.git>

Step 5: - Now change directory to “diva-apk-file” using “cd diva-apk-file”

Step 6: - Now decoding the “DivaApplication.apk” using “apktool d DivaApplication.apk”

Step 7:- After decoding complete go to “DivaApplication” Folder there you can see the application source code

**4) Demonstrate how vulnerability management process can be done using any tools like Qualys SSL Labs.**

Step 1: - open any browser and search Qualis SSL labs

Step 2: - go to www.ssc.com official website

Step 3: - click on the server test

enter any website URL

Step 4: - for example google.com or facebook.com

Step 5: - click on submit

Step 6: - it will show grade of the website which you have entered

Step 7: - after analyzing it close the website