Chapter 2: **IR, BC, DR - CC Exam Prep**

### 🚨 ****Incident Response (IR) Terms****

| **Term** | **Easy Explanation** |
| --- | --- |
| **Event** | Something noticeable on a system (like a login, alert, or crash). |
| **Incident** | A serious event that may harm data or system security. |
| **Breach** | When someone gets access to private data without permission. |
| **Intrusion** | An outsider breaking into a system without permission. |
| **Exploit** | A specific attack that takes advantage of a weakness. |
| **Threat** | Anything that could cause harm (like a hacker or virus). |
| **Vulnerability** | A flaw or weakness in a system that attackers can use. |
| **Zero Day** | A new flaw that no one knows about yet — no fix exists. |

### 🧯 ****Four Phases of Incident Response****

| **Phase** | **What It Means** |
| --- | --- |
| **Preparation** | Getting ready before an incident happens (training, tools, policies). |
| **Detection and Analysis** | Identifying and understanding the problem or attack. |
| **Containment, Eradication and Recovery** | Stopping the attack, removing it, and fixing the damage. |
| **Post-Incident Activity** | Reviewing what happened and improving for next time. |

### 👥 ****Types of Incident Response Teams (IRT)****

| **Model** | **Meaning** |
| --- | --- |
| **Leveraged** | Uses people from other departments when needed. |
| **Dedicated** | A full-time team focused only on incident response. |
| **Hybrid** | Mix of dedicated team + other staff when required. |

### 🔄 ****Business Continuity (BC) Terms****

| **Term** | **Easy Explanation** |
| --- | --- |
| **Business Continuity (BC)** | Keeping the business running even during big problems. |
| **Business Continuity Plan (BCP)** | A guide for what to do to keep running during a crisis. |
| **Business Impact Analysis (BIA)** | Finding out what parts of the business are most important and what happens if they stop. |

### 🧠 ****BCP Components (What’s in the Plan)****

Who’s on the response team and how to reach them

Steps to follow immediately during a crisis

Emergency contacts (e.g., vendors, customers)

How and when to start the plan

Checklists for actions and decisions

Call trees and alerts to notify people

### 💻 ****Disaster Recovery (DR) Terms****

| **Term** | **Easy Explanation** |
| --- | --- |
| **Disaster Recovery (DR)** | Restoring systems and IT services after a major problem. |
| **Disaster Recovery Plan (DRP)** | A detailed plan to fix and recover tech systems after a disaster. |

### 🛠️ ****DRP Components (What’s Inside the Plan)****

**Executive Summary** – Quick overview of the plan

**Department Plans** – Specific tasks for each part of the business

**Technical Guides** – Instructions for IT staff

**Full Copies** – Printed or digital versions given to team members

**Checklists** – Step-by-step instructions for recovery tasks

# Practice MCQs Based on Chapter 2

1. 1. What is the main goal of an Incident Response (IR) plan?

* A. To prevent disasters completely
* B. To stop hackers before they enter
* C. To detect and respond to incidents quickly
* D. To make sure systems are always available

✅ Correct Answer: C

1. 2. Which of the following is the correct order of the four main phases of Incident Response?

* A. Detection, Eradication, Preparation, Review
* B. Preparation, Detection and Analysis, Containment and Recovery, Post-Incident Activity
* C. Analysis, Backup, Response, Evaluation
* D. Monitoring, Defense, Reporting, Resolution

✅ Correct Answer: B

1. 3. A zero-day attack is best described as:

* A. An attack that lasts zero seconds
* B. An attack that has already been fixed
* C. An attack using an unknown vulnerability
* D. An attack that causes zero damage

✅ Correct Answer: C

1. 4. What is the purpose of a Business Continuity Plan (BCP)?

* A. To prevent all possible attacks
* B. To recover from a natural disaster
* C. To keep critical business operations running during a crisis
* D. To eliminate vulnerabilities in software

✅ Correct Answer: C

1. 5. Which of the following would most likely be part of a Disaster Recovery Plan (DRP)?

* A. Marketing strategy
* B. Password policy
* C. Technical guides for restoring IT systems
* D. Employee training manual

✅ Correct Answer: C

1. 6. What is a vulnerability?

* A. A software feature
* B. A detected attack
* C. A weakness that can be exploited
* D. A type of backup

✅ Correct Answer: C

1. 7. Who are typically part of the Incident Response Team (IRT)?

* A. Only top-level executives
* B. Only IT security staff
* C. A cross-functional group from impacted areas
* D. Only legal and HR departments

✅ Correct Answer: C

1. 8. An intrusion is defined as:

* A. A legal access to systems
* B. Accidental system failure
* C. Unauthorized access to a system or resource
* D. Update to the antivirus system

✅ Correct Answer: C

1. 9. Which of the following is not a component of a Business Continuity Plan (BCP)?

* A. Vendor contact details
* B. Call trees and alerts
* C. Antivirus signature updates
* D. Step-by-step response checklists

✅ Correct Answer: C

1. 10. What is the purpose of a Business Impact Analysis (BIA)?

* A. To block spam emails
* B. To test the firewall
* C. To find out which business processes are most critical
* D. To schedule staff meetings

✅ Correct Answer: C