Based on the provided Chapter 2 content, here are 20 multiple-choice questions focusing on incident response and business continuity/disaster recovery:

**Question 1**

Which of the following is the PRIMARY goal of incident management?  
 A) To minimize financial losses B) To be prepared C) To identify the attacker D) To document lessons learned

**Question 2**

What is the FIRST priority of any incident response?  
 A) Protecting business reputation B) Protecting life, health, and safety C) Identifying the source of the incident D) Containing the incident

**Question 3**

What is an incident in the context of information security?  
 A) Any observable occurrence in a network or system B) A weakness in an information system C) An event that actually or potentially jeopardizes the CIA of an information system D) A previously unknown system vulnerability

**Question 4**

What is the term for a security event where an intruder gains or attempts to gain access to a system without authorization?  
 A) Breach B) Vulnerability C) Exploit D) Intrusion

**Question 5**

Which of the following is NOT a typical phase in the incident response process?   
A) Preparation B) Detection and Analysis C) Containment D) Elimination

**Question 6**

Which phase of incident response includes developing a policy approved by management and identifying critical data and systems?  
 A) Preparation B) Detection and Analysis C) Containment D) Post-Incident Activity

**Question 7**

What is the primary intent of a business continuity plan?   
A) To identify vulnerabilities in an organization B) To recover from disasters only C) To sustain business operations while recovering from a significant disruption D) To respond to security incidents

**Question 8**

What is the name of the outlined document containing the business continuity plan? A) Green Book B) Red Book C) Blue Book D) Yellow Book

**Question 9**

Which of the following is NOT a common component of a business continuity plan?   
A) List of the BCP team members B) Notification systems for alerting personnel C) Source code for critical applications D) Guidance for management

**Question 10**

What is a Business Impact Analysis (BIA) used for?  
 A) To analyze the financial impact of a security breach B) To determine the attacker's identity C) To analyze system requirements and dependencies to determine future event priorities D) To calculate the cost of incident response

**Question 11**

What is the primary difference between Business Continuity and Disaster Recovery?   
A) Business Continuity maintains critical functions during disruption; Disaster Recovery restores everything to full operation B) Business Continuity is for natural disasters; Disaster Recovery is for cyber attacks C) Business Continuity is a short-term plan; Disaster Recovery is a long-term plan D) Business Continuity is for IT systems; Disaster Recovery is for physical facilities

**Question 12**

What is the end goal of a Disaster Recovery Plan (DRP)?  
 A) To identify the vulnerabilities that caused the disaster B) To restore the business to full last-known reliable operations C) To prevent future incidents D) To prosecute those responsible for the incident

**Question 13**

Which term describes a previously unknown system vulnerability that has potential for exploitation without risk of detection?  
 A) Zero Day B) Exploit C) Breach D) Threat

**Question 14**

What teams are commonly responsible for incident response in organizations?   
A) Red Teams B) Blue Teams C) CIRTs or CSIRTs D) Tiger Teams

**Question 15**

Which of the following is NOT a potential member of a typical incident response team?  
 A) Information security professionals B) Engineering representatives C) Customers D) Legal representatives

**Question 16**

During which phase of incident response would you isolate an attack?   
A) Preparation B) Detection and Analysis C) Containment D) Post-Incident Activity

**Question 17**

Which of the following is NOT a primary responsibility of a Security Operations Center (SOC)?  
 A) Determining the scope of damage caused by an incident B) Implementing recovery procedures C) Creating new security policies D) Supervising implementation of additional security measures

**Question 18**

What is the definition of a "breach" in information security?   
A) Any observable occurrence in a network or system B) The unauthorized disclosure or acquisition of personally identifiable information C) A deliberate security incident to gain access to a system D) A circumstance with potential to adversely impact organizational operations

**Question 19**

What should be included in the "Post-Incident Activity" phase of incident response?  
 A) Monitoring all possible attack vectors B) Choosing an appropriate containment strategy C) Documenting lessons learned D) Training staff on incident response

**Question 20**

What is one of the key components of a business continuity plan mentioned in the text?   
A) Employee personal information B) Communication strategies and backup contact methods C) Business competitors' information D) Source code repositories

**Answers and Explanations**

1. B - The text states "The primary goal of incident management is to be prepared."
2. B - The text clearly states "The priority of any incident response is to protect life, health and safety. When any decision related to priorities is to be made, always choose safety first."
3. C - According to the terminology provided, an incident is "An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits."
4. D - As defined in the terminology section, an intrusion is "A security event, or combination of events, that constitutes a deliberate security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization."
5. D - The phases mentioned in the incident response process are Preparation, Detection and Analysis, Containment, and Post-Incident Activity. "Elimination" is not mentioned as a standard phase.
6. A - The Preparation phase includes "Develop a policy approved by management" and "Identify critical data and systems, single points of failure."
7. C - The text states "The intent of a business continuity plan is to sustain business operations while recovering from a significant disruption."
8. B - The document is referred to as the "Red Book" in the text: "Red Book is an outlined document containing the business continuity plan."
9. C - Common components listed include BCP team members, response procedures, notification systems, and management guidance. Source code for applications is not mentioned as a component.
10. C - The text defines Business Impact Analysis (BIA) as "an analysis of information system's requirements, functions and inter dependencies used to assume a future event requirements and priorities in an disruption."
11. A - The text states "Business Continuity which maintains the operation of critical business functions. Whereas, Disaster Recovery is about recovering everything back to full operation."
12. B - The text states the end goal of DRP is "to see the business restored to full last-known reliable operations."
13. A - According to the terminology section, Zero Day is "A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures or methods."
14. C - The text states "These teams are commonly known as computer incident response teams (CIRTs) or computer security incident response teams (CSIRTs)."
15. C - The text lists potential members including senior management representatives, information security professionals, legal representatives, public affairs representatives, and engineering representatives. Customers are not mentioned as typical team members.
16. C - The Containment phase includes "Isolate the attack" as one of its components.
17. C - The text lists the primary responsibilities of an SOC as determining damage scope, determining if confidential information was compromised, implementing recovery procedures, and supervising implementation of additional security measures. Creating new security policies is not listed.
18. B - According to the terminology section, a breach is defined as "The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information..."
19. C - The Post-Incident Activity phase includes "Document lessons learned" as one of its components.
20. B - The text lists "List of the BCP team members, including multiple contact methods" and mentions "A key part of the plan is communication, including multiple contact methodologies and backup numbers."