

EC-Council

INCIDENT RESPONSE

C | C T

Certified Cybersecurity Technician


Module - 19

Incident Response

This page is intentionally left blank.

Module Objectives

- 01 Understanding the Concepts of Incident Response
- 02 Understanding the Role of the First Responder in Incident Response
- 03 Understanding the Incident Handling and Response Process
- 04 Overview of Various Phases Involved in Incident Handling and Response



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

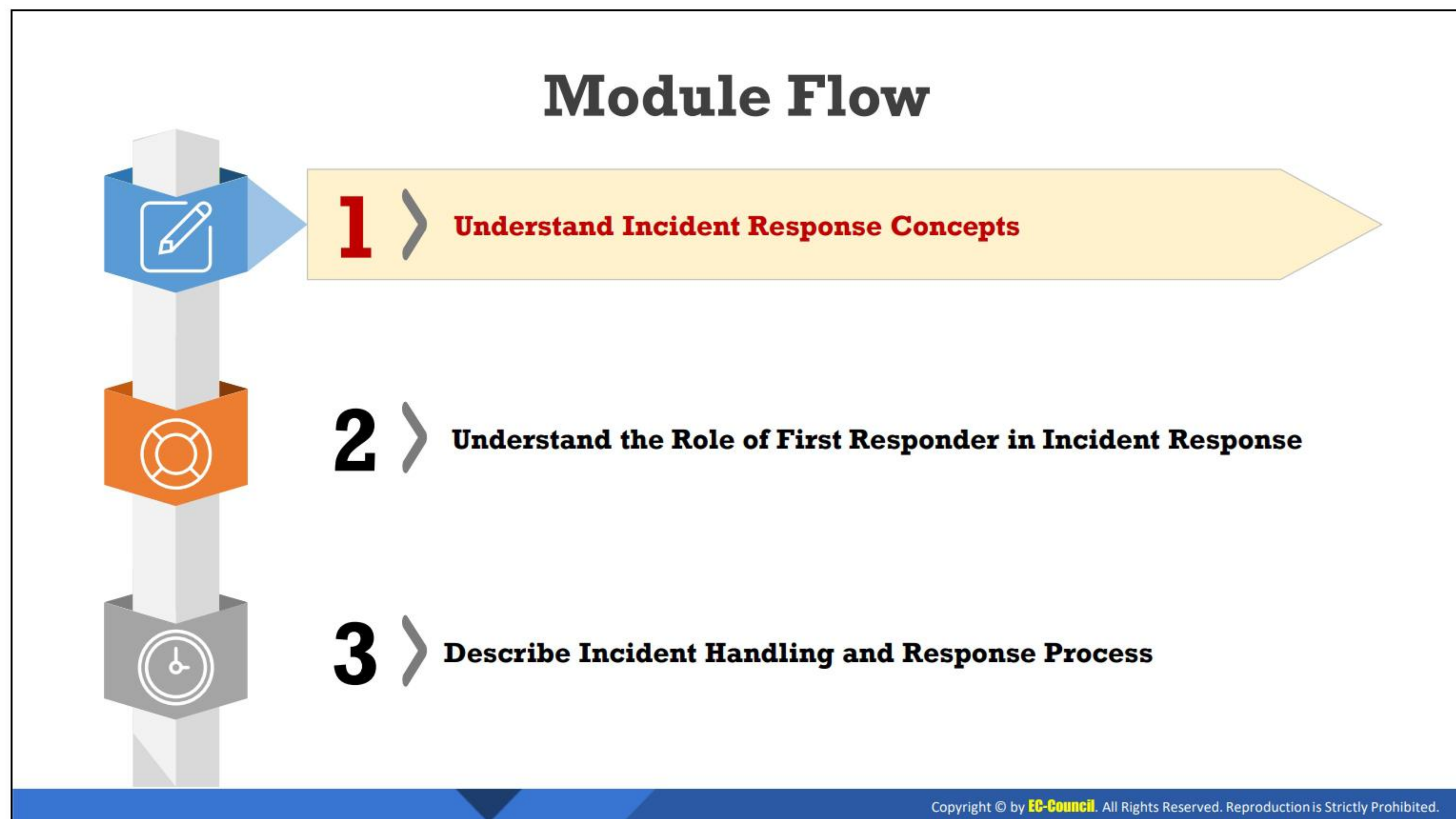
Module Objectives

Information security incidents have skyrocketed in recent years, owing to the adoption of digital technologies and the daily innovation of new technologies. In this environment, organizations are at risk of suffering huge losses related to data, trust, profits, systems, devices, and human resources. Therefore, it is crucial for organizations to be ready to battle—if not completely prevent—these incidents.

This module will help in understanding the complete incident handling and response process that organizations must institute to face, fight, and prevent different types of information-based attacks.

At the end of this module, you will be able to do the following:

- Define the concept of incident response
- Understand the role of the first responder in incident response
- Explain the incident handling and response process
- Understand various phases involved in incident handling and response



Understand Incident Response Concepts

Understanding the concept of incident response (IR) will help handle security breaches effectively and minimize the damages from a cybersecurity attack. The objective of this section is to help you understand the approach, goals, and advantages of IR. It will highlight the roles and responsibilities of an incident handling and response team.

Incident Response

- 01 Incident response (IR) is the process of taking **organized** and **careful** steps when reacting to a security incident
- 02 It involves a sequence of steps that begin with first **identifying** and **reporting** an incident
- 03 IR processes differ from organization to organization according to their business and operating environment
- 04 The **Incident Handling and Response Team** is a group of specialized people who collectively **respond**, **remediate**, **mitigate**, **recover**, and **communicate** the impact of incidents involving computer security breaches
- 05 The IH&R team works on an **incident response plan** when dealing with a security incident



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Response

Incident response (IR) is the process of taking organized and careful steps when reacting to a security incident. It involves a sequence of steps that begin with first identifying and reporting an incident. IR is a systematic approach that is adopted to handle security incidents with minimal damage, recovery time, and costs. In the process of responding to an incident, information such as the vulnerability of the network that caused the attack to occur, who initiated the attack, and the kind of devices and files that are affected are known. IR processes differ from organization to organization according to their business and operating environment.

The incident handling and response team is a group of specialized people who collectively respond, remediate, mitigate, recover, and communicate the impact of incidents involving computer security breaches. The IH&R team works on an incident response plan when dealing with a security incident.

Goals of IR

- To detect if an incident occurred and if it is an actual security incident or a false positive
- To maintain or restore Business Continuity
- To reduce the impact of an incident
- To analyze the cause of an incident
- To prevent future attacks or incidents
- To improve security and incident response
- To prosecute illegal activity

Advantages of IR

- Equips the organization with safe procedures to be followed when an incident occurs
- Saves time and effort, which is otherwise wasted when fixing an encountered incident
- Helps the organization learn from past experiences and recover from losses more quickly
- The skills and technologies required to tackle an incident are determined in advance.
- Saves the organization from legal consequences arising from a severe incident
- Helps determine similar patterns across incidents and handle them more efficiently

Roles and Responsibilities of IH&R Team



Depending on the organization, an **in-house** or an **external IH&R team** holds different titles, roles, and responsibilities for an incident response

Management

- ❑ An individual or group of individuals from the management with leadership and **decision-making** authority

Information Security Team

- ❑ An individual from the information security team who has experience in **discovering** and containing **incidents**

IT Staff

- ❑ An individual who is aware of the information system and **network areas**. They may be system or network administrators

Physical Security Staff

- ❑ An individual who is responsible for **physical security** and identifying the extent of any damage

Attorney

- ❑ An individual responsible for providing **legal advice**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Roles and Responsibilities of IH&R Team (Cont'd)

HR Representative

An individual responsible for handling **employee issues** for an employee involved in an incident

PR Specialist

An individual responsible for conveying **company details** after an incident

Financial Auditor

An individual who assesses the **financial loss** to a company from an incident

IR Officer

An individual responsible for all actions of the **IR Team and IR Function**. They may be an executive-level employee such as a CISO, or another corporate representative

IR Manager

An individual who receives the **initial IR alerts** and leads the IH&R team in all IR activities

IR Assessment Team

A group of individuals who make decisions on the classifications and the **severity** of the incident identified. The team comprises representatives from IT, Security, Application, Support, and other business areas

IR Custodians

An individual responsible for the **remediation and resolution** of the incident that occurred. They include technical experts and application support representatives.

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Roles and Responsibilities of IH&R Team

The IH&R team is a group of specialized people who collectively respond to, investigate, remediate, mitigate, and communicate the impact of incidents involving computer security breaches. The IH&R team plays a very important role in the organization. However, maintaining such a team separately can involve huge costs and other resources. Therefore, organizations generally use their current employees who are experts in their fields to constitute the IH&R team in addition to a few dedicated members.

The IH&R team can include persons including network and system administrators, managers, stakeholders, employees, and security operations center analysts.

Typical roles and responsibilities of IH&R team members may vary based on the organization's IR activities.

- **Management:** In an organization, the management includes the top-most authoritative decision makers. It may include a single entity or a group of entities who make decisions when an incident occurs. The management should be the first entity to learn about an incident. They decide the steps to be taken after the occurrence of an incident is confirmed.
- **Information Security Team:** The team consists of a group of individuals who possess the skills to detect and analyze security incidents. They can easily identify the nature, category, and scope of the incident.
- **IT Staff:** IT Staff comprises the individuals who are either system or network administrators. They detect the incident by analyzing network traffic, system logs, and service packages and patches, among others, and report it to the management or the IH&R team. They execute the first response step to avoid further damage.
- **Physical Security Staff:** Physical security staff contribute to the handling of and response to physical security incidents. They can also be the first responders to a physical security incident. They actively report the occurrence of a physical security incident such as fire, theft, damage, and unauthorized access to the management.
- **Attorney:** The attorney is a legal advisor for the organization. Attorneys play a major role in ensuring that any evidence collected is admissible in a court of law. They can also help an organization recover from a financial loss due to an incident.
- **HR Representative:** An internal employee may be involved in a security incident. In these situations, Human Resources (HR) becomes involved when the IH&R team detects that an internal employee is involved in the security incident. HR provides the IH&R team with the best possible solution for dealing with any employee involved in an incident.
- **PR Specialist**

The Public Relations (PR) department serves as a primary contact for the media and informs the media about an event. They update the website information, monitor media coverage, and are responsible for stakeholder communication, including to the following:

- Board
- Foundation personnel
- Donors
- Suppliers/vendors

- **Financial Auditor**

Financial Auditors are individuals who assess the financial loss of the organization after an incident. The auditor is responsible for accounting for all losses that occurred as a result of the incident. The auditor is responsible for reporting the financial imbalance in the organization's account.

- **IR Officer**

The IR Officer is an individual who oversees all IR activities in an organization. IR officers are executive employees who are responsible for how the IH&R team functions. Every action taken by the IH&R team is reported back to the IR Officer who further reports to the management of the organization.

- **IR Manager**

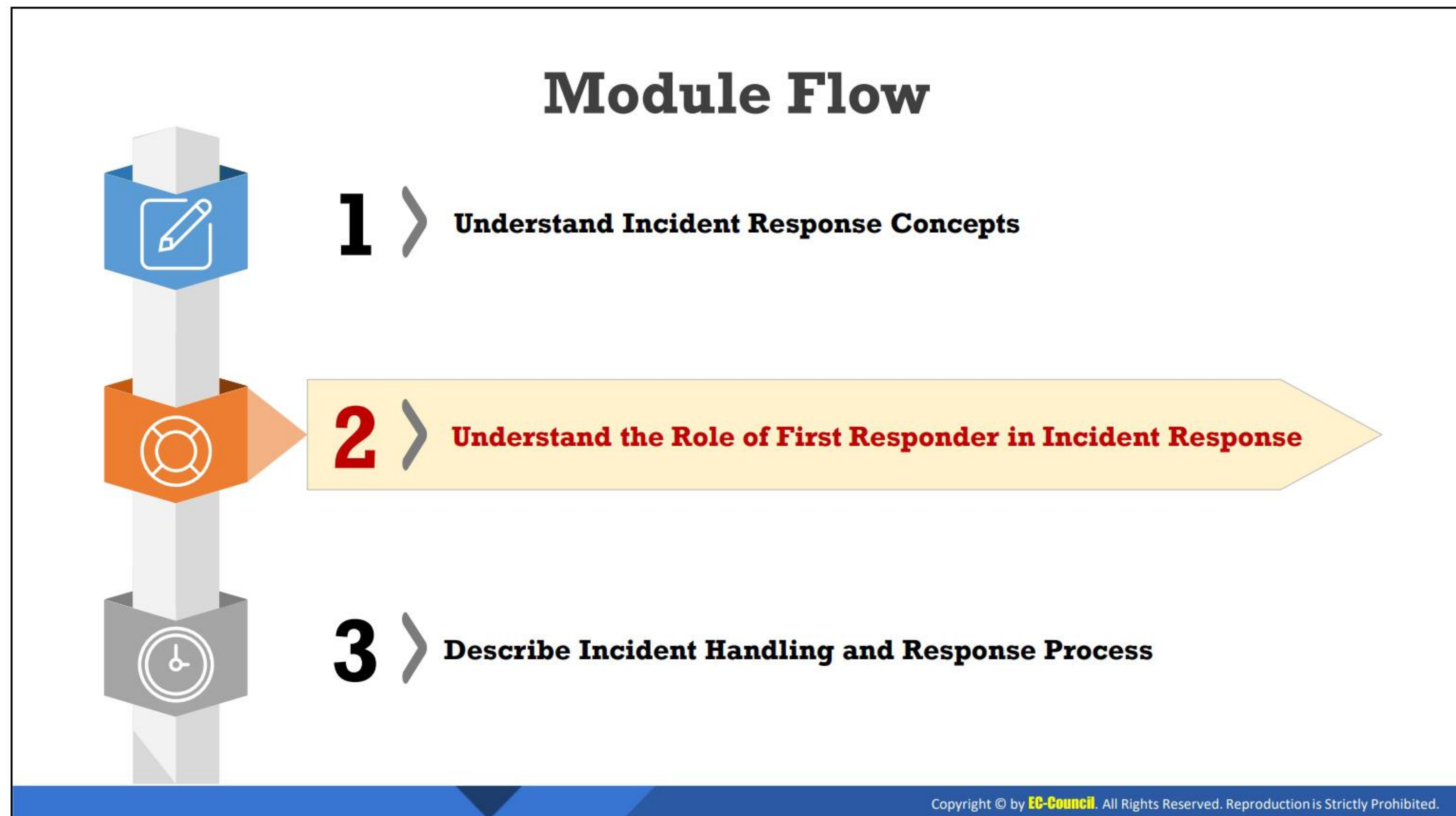
The IR Manager must be a technical expert who understands security and incident management. The IR Manager focuses on the incident and analyzes how to handle it from a management and a technical point of view. They are responsible for the actions performed by the incident analysts and reporting the information to the IR Officer.

- **IR Assessment Team**

The IR Assessment Team comprises individuals who prioritize the occurrence of an incident based on the amount of loss it caused to the organization. The team comprises individuals from various domains such as IT, security, application support, and other business areas.

- **IR Custodians**

IR Custodians are either technical experts or application support representatives. They play an important role when an application incident occurs. To respond to the incident, IR Custodians create an action framework that is further shared with the management.

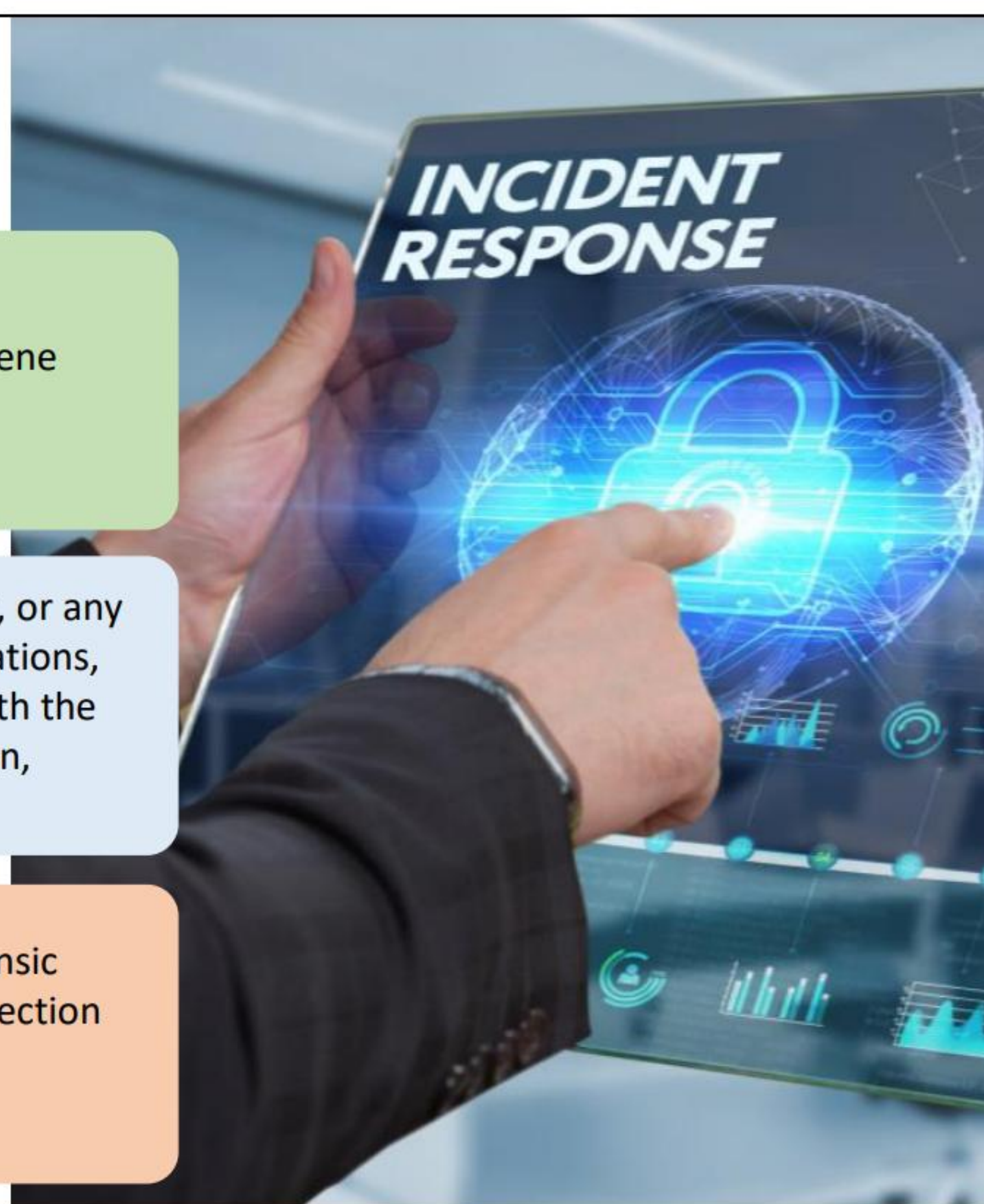


Understand the Role of First Responder in Incident Response

The objective of this section is to understand the role of the first responder in incident response (IR). The first responder plays a crucial role by providing a quick initial response to the incidents of threats or attacks in the organization. This section deals with the roles and responsibilities of the first responder.

First Responder

- ❑ A first responder is an individual who arrives first at the crime scene and **brings the incident to the attention of others**
- ❑ The first responder could be an end user, network administrator, or any other individual who is involved in the day-to-day network operations, spends a lot of time in **network environments**, and is familiar with the organization's assets, network traffic, performance and utilization, network topology, location of each system, security policy, etc.
- ❑ The first responder play a **key role** in incident response and forensic investigation process. He/she can provide great help in early detection of incident, source of the incident, impact of incident, evidence collection and preservation, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

First Responder

The IH&R team works on the pretext of the first responder of the incident. The term “first responder” refers to the individuals who arrive first at the crime scene and gain access to the victim’s computer system after the incident report. A first responder may be a user, network administrator, law enforcement officer, or investigation officer. They are responsible for protecting, integrating, and preserving any evidence obtained from the crime scene. The first responder plays a key role in incident response and forensic investigation process. He/she can provide great help in early detection of incident, source of the incident, impact of incident, evidence collection and preservation, etc.

The time gap between the occurrence of an incident and transference of evidence is an important aspect in incident response. It is the responsibility of the first responder to ensure the reliability and liability of the evidence. The method used by any first responder is very important in preserving the evidence and finding the attackers. First responders should be trained to gather evidence without modifying any of the services running at that moment. This is a critical task for the first responders as they have to gather evidence before it is lost. The first responder needs to have a dedicated and well-organized plan when responding to any type of incident as they collect the initial information and determine the extent and impact of the attack or incident. This allows other people involved in handling the incident to effectively determine other courses of action that may be required for investigating the incident.

The first responder should be aware of the incident response and forensics investigation procedure, otherwise response to the incidents can be delayed. The delay in incident response can increase the potential impact of incident or even evidence can be corrupted and/or lost. An experienced first responder can easily apply good forensic techniques when they respond to an incident in the initial stages. They can predict the extent to which any change in the evidence

may affect the further investigation. This proficiency is an extra add-on in maintaining the availability, integrity, and reliability of the evidence. The first responder needs to always understand the importance of their role as it highly affects the security and efficiency of the organization.



First Responder Roles and Responsibilities

- 👍 **Reporting** the incident
- 👍 **Alerting** the management and incidence response teams
- 👍 **Containing** incident
- 👍 **Identifying** the crime scene
- 👍 **Collecting** the complete information about the incident
- 👍 **Protecting** the crime scene
- 👍 **Documenting** all the findings
- 👍 **Preserving** temporary and fragile evidence
- 👍 **Packaging** and transporting the electronic evidence

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

First Responder Roles and Responsibilities

- Reporting the incident
- Alerting the management and incidence response teams
- Containing incident
- Identifying the crime scene
- Collecting the complete information about the incident
- Protecting the crime scene
- Documenting all the findings
- Preserving temporary and fragile evidence
- Packaging and transporting the electronic evidence

First Response Rule

- Under no circumstances should anyone except forensic analysts make any effort to collect or recover the data from any computer system or electronic device that holds electronic information.
- Remember that any information present inside the collected electronic devices is probable evidence and should be treated accordingly.
- Any attempts to retrieve data by unqualified individuals should be avoided. These attempts could either compromise the integrity of the files or result in the files becoming inadmissible in legal or administrative proceedings.
- The workplace or office must be secured and protected to maintain the veracity and quality of the crime scene and the electronic storage media.



Things to Know before First Response

The first responder should review the incident plan of their organization and suggest or implement changes to the incident response plan (IRP) as required.

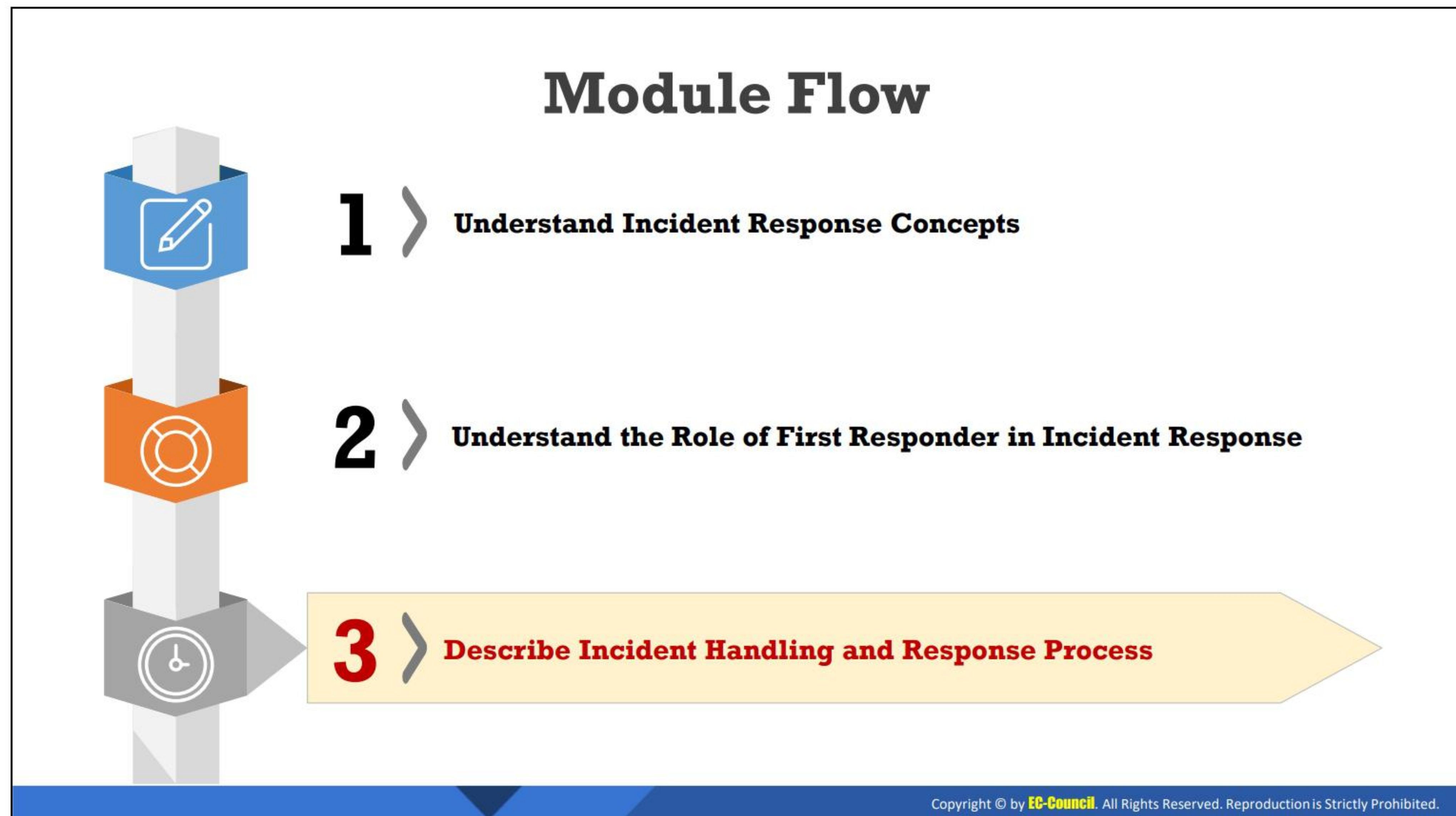
A typical IRP includes the following:

- **Contacts of IH&R Team:** It will help a first responder to immediately contact the IH&R team when an incident occurs. Having an IH&R team immediately on the location of the incident will help minimize any delay in responding to an incident.
- **Escalation procedures:** First responders should know whom to contact and report the incident. There will be certain escalation procedures for the first responder that will help them report the incident without any delay.

First responders collect and document the following information before escalating the incident:

- IP address and physical location of the affected systems
- Type of data on the systems
- Timeline of activities the system/user went through before the incident
- How the incident was detected
- Number of users affected
- **Procedure for reporting and handling an incident:** First responders should be aware of reporting and IR procedures.

- **Containment actions:** The IRP includes containment actions for all types of security incidents. Different containment actions are required for different types of incidents. The first responder should be aware of the containment actions for various types of security incidents, as it helps prevent further damage to an organization.



Describe Incident Handling and Response Process

“Incident handling and response” (IH&R) is the practice of managing the processes involved in responding to an incident—such as preparation, detection, containment, eradication, and recovery—to overcome the impact of an incident quickly and efficiently. The objective of this section is to introduce you to the complete incident handling and response (IH&R) process.

Importance of IH&R Process

- ❑ Incidents can happen **any day**, at **any time** and can **compromise crucial business data** leading to heavy losses, in terms of both finance and reputation
- ❑ With the rapid increase in threats and incidents, the need for **effective** and **structured** incident handling and response has become mandatory for every organization



Purpose of IH&R process is to:

- ✓ Protect networks and systems
- ✓ Ensure timely incidents handling
- ✓ Ensure the gathering of appropriate information
- ✓ Identify false positives
- ✓ Efficiently use resources

- ✓ Address legal issues
- ✓ Comply with local, national, and international guidelines
- ✓ Train and protect personnel
- ✓ Develop comprehensive documentation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Importance of IH&R Process

The exponentially rapid progress of technology for organizations has given rise to new technologies capable of serving diverse sectors. However, this technological diversity has notably intensified the frequency, diversity, severity, and approach of security threats, indicating the need for every organization to mandate effective and structured IH&R processes.

Incidents that can compromise crucial business data and cause heavy financial and reputational losses can happen on any day and at any time. To avoid such losses, organizations should prepare to efficiently handle any incidents.

Organizations therefore employ the IH&R process to:

▪ Protect Networks and Systems

With technology continuously evolving, attackers are finding new ways to damage businesses. In such a scenario, it is difficult to completely secure systems and data even after instituting expensive high-level security features such as special access controls on various computing resources. The best strategy for securing computer systems and protecting networks is to quickly detect any indicators of compromise and recover from the security incident. An efficient IR procedure ensures the proper maintenance of all critical business operations during and after an incident.

▪ Ensure Timely Incident Handling

During any incident situation, time is the most important factor: as time increases, damage increases. Therefore, IH&R processes should always encourage organizations to adopt various time management techniques and tools for detecting, validating, and containing incidents before it is too late.

- **Ensure the Gathering of Appropriate Information**

The IH&R process ensures the gathering of appropriate and accurate information necessary for understanding a security incident, building an IH&R team from existing employees, clarifying standard security procedures, developing knowledge of required tools, and deploying the latest security measures to handle any future information security incidents.

- **Identify False Positives**

Detecting an incident is an arduous process; however, it becomes even more difficult when it is necessary to identify false positives—even simple mistakes, such as application program errors, human errors, hardware failure errors, and system configuration errors, can generate alarms. IR processes crucially help organizations differentiate actual incidents from false alarms and advise best practices for handling both.

- **Efficiently Use Resources**

The technical and managerial resources required for incident handling are often limited. The best way to use these resources is to respond to incidents as quickly as possible. Information gained during the incident handling process can help to prevent incidents or enhance an organization's ability to handle future incidents and implement strong security for systems and data.

- **Address Legal Issues**

Organizations must abide by the laws of their jurisdictions when dealing with security incidents; otherwise, they may face legal issues. Sometimes, for example, incident handling requires the investigation of private information, and such processes can conflict with individual privacy rights—according to the U.S. Department of Justice, it is illegal for organizations to use certain monitoring techniques to identify an information security incident. To be sure, then, IH&R processes must comply with different laws and acts, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA). Moreover, IH&R processes should also be sure to advise incident responders to attain proper permissions and approvals from concerned authorities. In addition, IH&R processes may also define a strategy for identifying and prosecuting the perpetrators of security incidents. The key takeaway here is that aligning incident procedures with relevant laws fortifies an organization against legal and public liabilities.

- **Comply with Local, national, and International Guidelines**

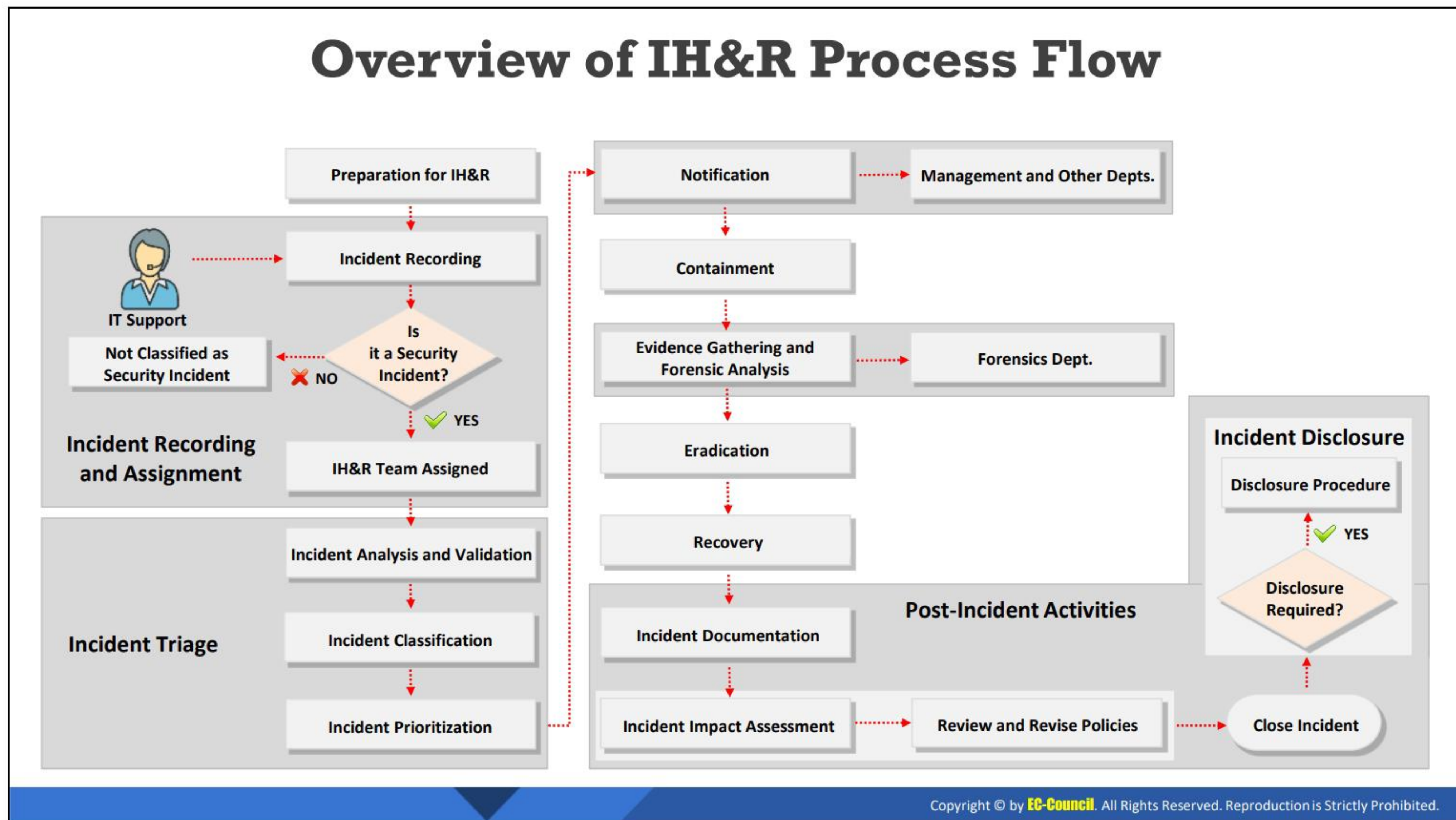
An IH&R process can help an organization comply with local and international protocols, policies, control measures, and guidelines set by various Community Emergency Response Teams (CERTs), while at once enabling it to handle and recover from any type of information security incident.

- **Train and Protect Personnel**

A good IH&R process requires an organization to build a good team capable of accelerating analysis, limiting damage to a minimal level, completely eradicating the incident, and restoring operations. This team will also help the organization learn from the incident and implement such knowledge to improve network safety. A swift IR helps to protect an organization's human resources from any physical consequences of a workplace incident.

- **Develop Comprehensive Documentation**

IH&R processes must advise the documentation of the whole scenario starting from the alert generation to the identification of the best solution to the incident. This documentation will serve as a reference for analyzing the mistakes, threats, or vulnerabilities that paved the way for the incident and will thus offer insights helpful for future prevention, especially when they inform which advanced security measures may best prevent future attacks.



Overview of IH&R Process Flow

IH&R combines various cybersecurity processes under a single procedure for combating incidents, quickening responses, improving controls and management processes, easing communication, improving resource use, evenly distributing tasks, efficiently reporting incidents and responses, and so on. Incident handling is like fighting a war, but on the cyber front.

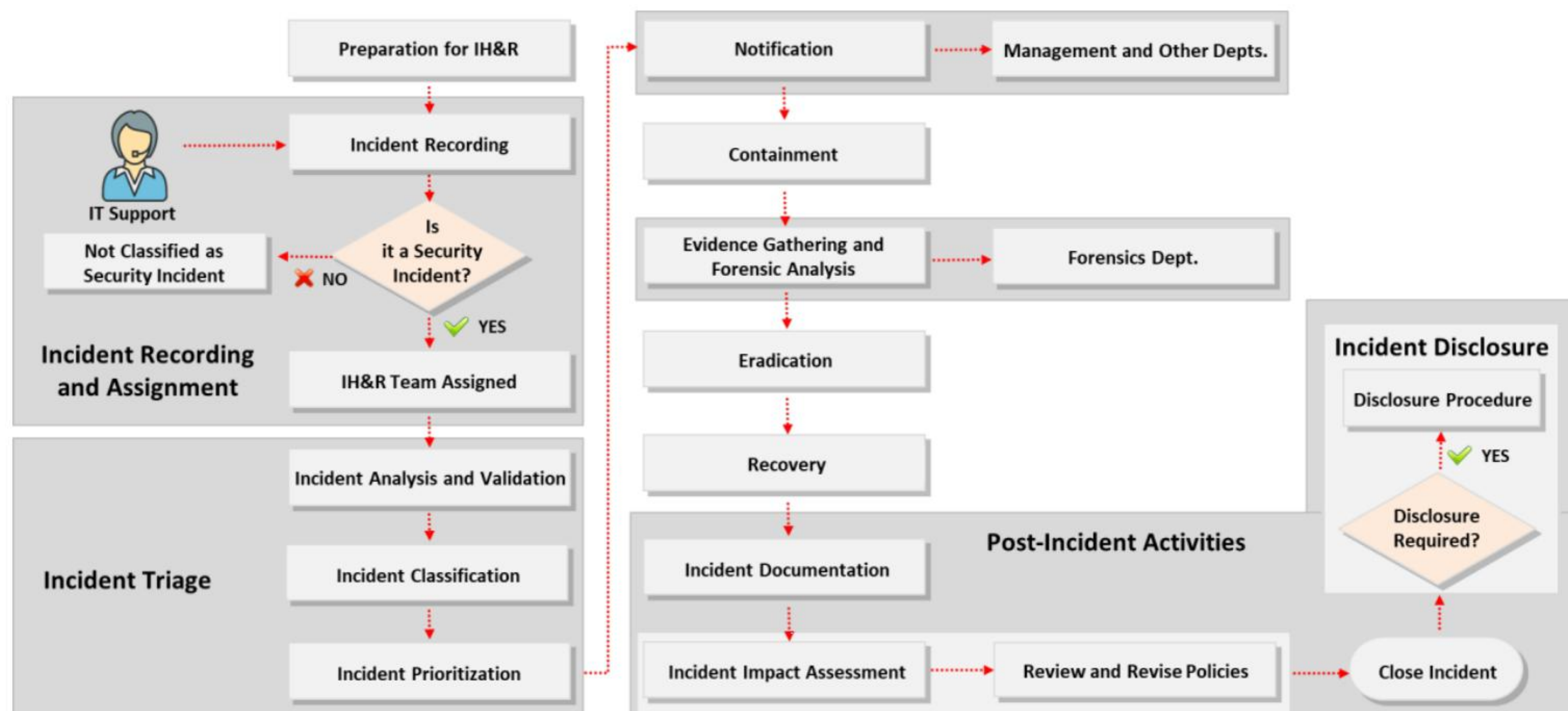


Figure 19.1: IH&R process flow

- **Step 1: Preparation for IH&R**

The first phase of IH&R is to prepare to face the security issue(s). Preparation includes auditing the resources and assets to determine the purpose of the security response; defining the rules, policies, and procedures that drive the IH&R process; building and training an IR team; defining incident readiness procedures; gathering required tools; and training employees to secure their systems and accounts.

- **Step 2: Incident Recording and Assignment**

The preparation phase is followed by an incident recording and assignment phase that involves the initial reporting and recording of the incident. This phase includes identifying the incident and defining a proper incident communication plan for employees—notably, this latter element can include normalizing communication methods that involve informing IT support personnel or raising an appropriate ticket. When a user or an employee reports any suspicious behavior on his or her system to IT support staff, a ticket or token is created about the irregular behavior and a member from the IR team is assigned to analyze the issue. Based on the ticket or the IT professional's intimation, the IH&R team will look into the issue and, if the issue qualifies as an incident, an IH&R team will be assigned to handle the incident, with the compromised device sent to the IH&R team for further investigation. Otherwise, the issue will be considered resolved and the ticket will be closed.

- **Step 3: Incident Triage**

In this phase, the incident will be analyzed, validated, categorized, and prioritized. The IH&R team will further analyze the compromised device to find incident details, such as the attack's type, severity, target, impact, and method of propagation as well as the vulnerabilities the attacker exploited. These details help the IH&R team to scale its impact and determine what other targets were involved in the incident, what techniques it must apply to contain the incident, and what it must prioritize to solve the incident.

- **Step 4: Notification**

The notification phase involves the release of incident information to various stakeholders, including management, third-party vendors, and clients. The notification phase occurs as soon as the incident is confirmed and validated, with the incident handlers first communicating the issue to management to gain necessary approvals and permissions.

- **Step 5: Containment**

The containment phase—which occurs at the same time as the notification phase—involves the IH&R team's containment of the incident. Crucially, the containment phase must be performed to stop the infection from spreading to other organizational assets. Along these lines, the important take away here is that the containment phase helps an organization stop a live attack from spreading and reduce damage and losses.

- **Step 6: Evidence Gathering and Forensic Analysis**

The evidence gathering phase occurs after the containment phase and involves the IH&R team collecting evidence. In this phase, the team will accumulate all possible evidence related to an incident and submit it to the forensic department for investigation. Such evidence may include details related to the method of attack as well as the vulnerabilities exploited, security mechanisms averted, network devices infected, and applications compromised that may have acted as pathways in the attack. Collecting and analyzing this information helps the IH&R team to block propagation methods to eradicate the incident and prevent it from reoccurring in the future.

- **Step 7: Eradication**

The eradication phase involves the IH&R team removing or eliminating the root cause of an incident and closing all attack vectors to prevent similar incidents in future. Eradication methods may include patching vulnerabilities, replacing malfunctioning devices, and installing better security mechanisms, including those that scan for malware signatures.

- **Step 8: Recovery**

After eliminating the causes of an incident, the IH&R team is responsible for restoring the affected systems, services, resources, and data through a recovery process. It is the responsibility of the IR team to ensure—to the extent possible—that the incident does not disrupt the organization's operations. Therefore, the IH&R team may need to recover compromised devices, applications, systems, or terminals as soon as possible by either replacing them or quickly fixing the issue.

- **Step 9: Post-Incident Activities**

This stage occurs only after the incident has been contained and the systems recovered. All tasks performed by IH&R personnel after this stage—such as incident documentation, incident impact analysis, policy review and revision, and incident disclosure—qualify as “post-incident activities.”

- **Incident Documentation**

Incident responders must document the complete IH&R process from detection to recovery. Such documentation will serve as a future reference to facilitate understanding of the practices employed to handle the incident. Notably, handlers should present the report to legal counsel; submit it to management; and use it to assess loss, review policies, change security norms, and reframe user protocols to improve network security.

- **Incident Impact Assessment**

After completing the formal IH&R process from incident recording through documentation, the IH&R team will analyze all information available to perform an incident impact analysis that assesses the impact of the damages or losses the organization suffered as a result of the incident.

- **Policy Review and Revision**

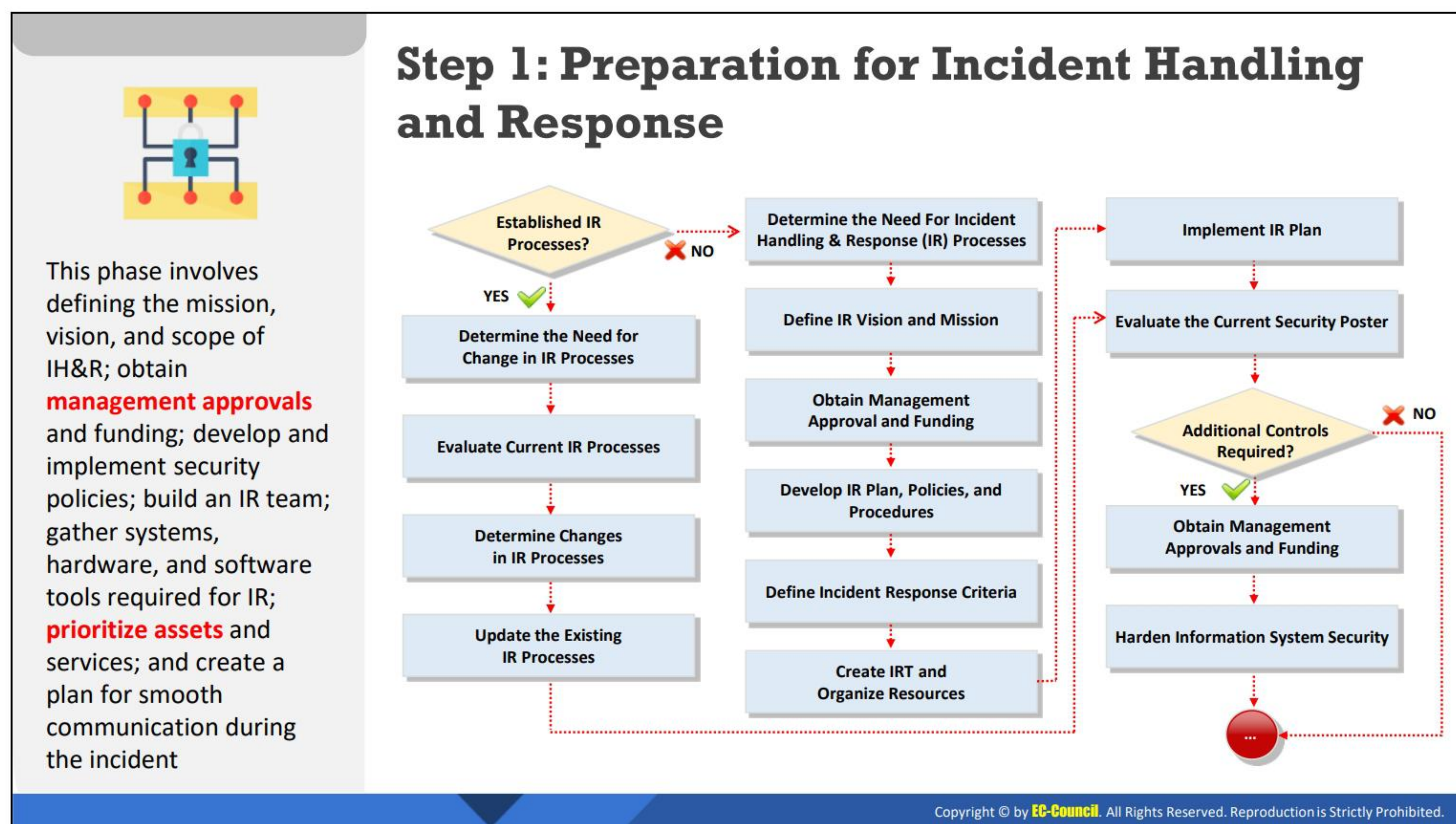
After assessing the incident's impact, the IH&R team will review and revise the organization's policies, preparation and protection procedures, and security controls to prevent future incidents. They will also share the identified threat information with threat intelligence teams.

- **Closing the Investigation**

By this phase, the incident will have been thoroughly investigated and documented and appropriate policies will have been reviewed and revised. This phase involves the official termination of the investigation and the planning of the implementation of the incident evidence retention policy.

- **Incident Disclosure**

After formally closing the incident, the organization's IH&R team and management will discuss whether to disclose the incident's details to the public (e.g., customers, media, industry intelligence). Additionally, the incident handlers are also responsible for communicating the issue to other departments in the organization (e.g., legal, human resources, forensics).



Step 1: Preparation for Incident Handling and Response

Preparation is the first and most important phase in the incident handling process; it enables an organization to establish an efficient IR process. In this stage, the organization will assess its assets, organizational structure, security policies, services, requirements for incident procedures, and other crucial elements of incident handling. Crucially, this stage enables organizations to take precautionary measures before an incident occurs; thus, the success of an IR process depends on the preparation phase.

In this stage, the organization will define the mission, vision, and scope of IH&R; obtain management approvals and funding; develop and implement security policies; build an IR team (a team of experts capable of handling any computer security incidents); gather systems, hardware, and software tools required for IR; prioritize assets and services; and create a plan for smooth communication during the incident.

Preparation is the readiness to respond prior to the actual occurrence of an incident event. Requirements for preparation include the following.

- Establishing a reasonable group of defense/controls depending on the threats posed on the following:
 - Open systems that are vulnerable to attacks
 - Secured systems with no IR
 - Systems dealing with incidents that are to be secured
- Developing a group of methods to deal with incidents:
 - Measures to be considered in different situations by the staff

- Contact information
- Keeping information from other neighboring organizations
- Assigning people to participate in the IR effort
- Determining risk levels and limits
- Acquiring resources and people to solve problems:

Monetary resources are required for hardware, software, training, and special equipment for analysis and forensics. Examples of resources include PDAs, safe vaults, Intrusion Detection System (IDS) software, and database server software.
- Developing an infrastructure that supports IR:

The overall business strategy should be developed to incorporate mechanisms into processes in order to respond to incidents.

 - Line of authority and management should be in place.
 - Defenses/controls specifically matching the resources of the network must be chosen.
 - IR procedures must be followed effectively.
 - Resources should be provided with proper finances.
 - Contact details should be maintained.
 - Evidence of IRs are to be stored.
 - Legal issues should be appropriately addressed.
 - System administrators are responsible for the preparation stage. Their responsibilities include the following:
 - Ensuring password policies
 - Disabling default accounts
 - Configuring appropriate security mechanisms
 - Executing and enabling system logging and auditing
 - Patch management
 - Ensuring proper backups
 - Ensuring the integrity of file systems
 - Identifying abnormal behavior in the system

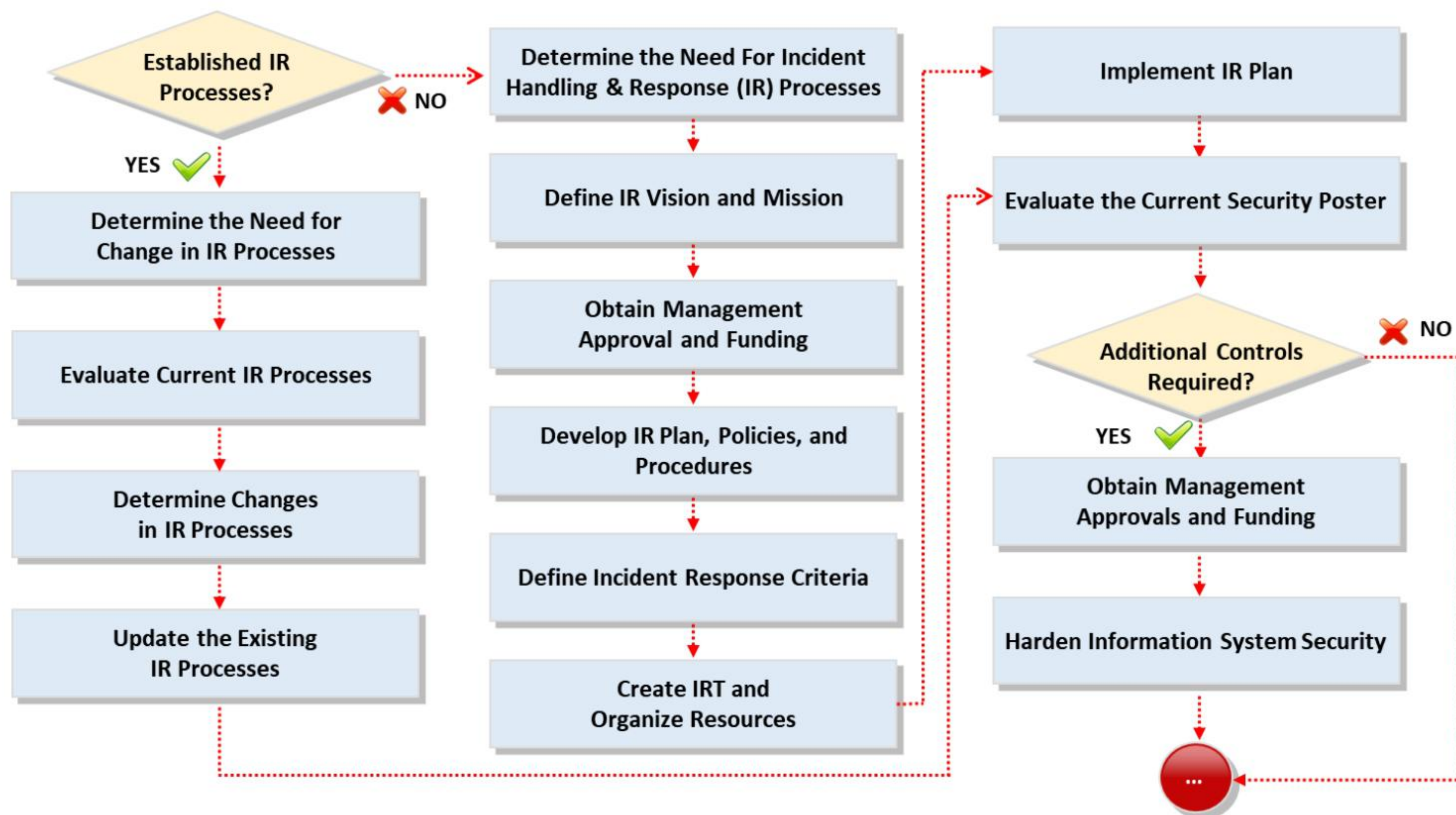


Figure 19.2: IH&R preparation phase—process flow

Incident Response Plan

The IR plan determines the **future course of action** for establishing, managing, and strengthening incident response capabilities

IR plan should:

- Address the mission and vision statements
- Meet the goals of incident response initiative
- Comply with the statement of senior management approval
- Include strategies to achieve set goals and timelines
- Have an organized approach to incident response
- Identify incident response key performance indicators that organization can use for future reference
- Provide a statement of interoperability
- Add value to other organizational processes
- Make efficient use of all the resources
- Strengthen the organization's security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Response Plan

The IH&R creates an incident response plan (IRP) before handling and responding to the incidents. An IRP is a set of guidelines that are required when responding to an incident in a dedicated and formal manner. The IR plan determines the future course of action for establishing, managing, and strengthening incident response capabilities. The plan contains the elements required for executing the IR effectively. These plans include response instructions for any detected incidents. The IRP includes the company requirements such as size, structure, and functions. The plan identifies the resources required for managing the incidents.

- IR plan should:
 - Address the mission and vision statements
 - Meet the goals of incident response initiative
 - Comply with the statement of senior management approval
 - Include strategies to achieve set goals and timelines
 - Have an organized approach to incident response
 - Identify incident response key performance indicators that organization can use for future reference
 - Provide a statement of interoperability
 - Add value to other organizational processes
 - Make efficient use of all the resources
 - Strengthen the organization's security

- An IRP should include the following:
 - Aim of the IRP
 - Objectives and approaches
 - Methodology of the IR
 - Standards to assess IR efficiency
 - Observing the current status of IR
- Components of an IRP:
 - Name and contact information of the IH&R team
 - System details such as data flow diagrams and network diagrams of the incident
 - The complete process required while recording and handling an incident
 - Report security incidents to the Information Security and Policy (ISP), who appoints a security analyst to handle the incident
 - Respond to the incident in a timely manner

Training and Preparing IH&R Personnel

- ❑ Maintain **sufficient overall staff** so that the team members have **uninterrupted** work time
- ❑ Provide **hardware** and **software** components
- ❑ Provide the team with appropriate **technical references**
- ❑ Prepare a **training budget** to maintain, enhance, and **increase proficiency** in technical areas and security disciplines, including the **legal aspects** of the incident response and updates to regulations
- ❑ Hire **external** subject matter experts for training



- ❑ Rotate team members through incident response team tasks to build confidence in various roles
- ❑ Develop a **mentoring program** for senior technical staff to train less experienced staff regarding the incident handling process
- ❑ Develop various **scenarios on incident handling** and conduct roundtable discussions on responses
- ❑ Conduct training and incident handling **mock drills** and **practice sessions** to make the teams familiar with the process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

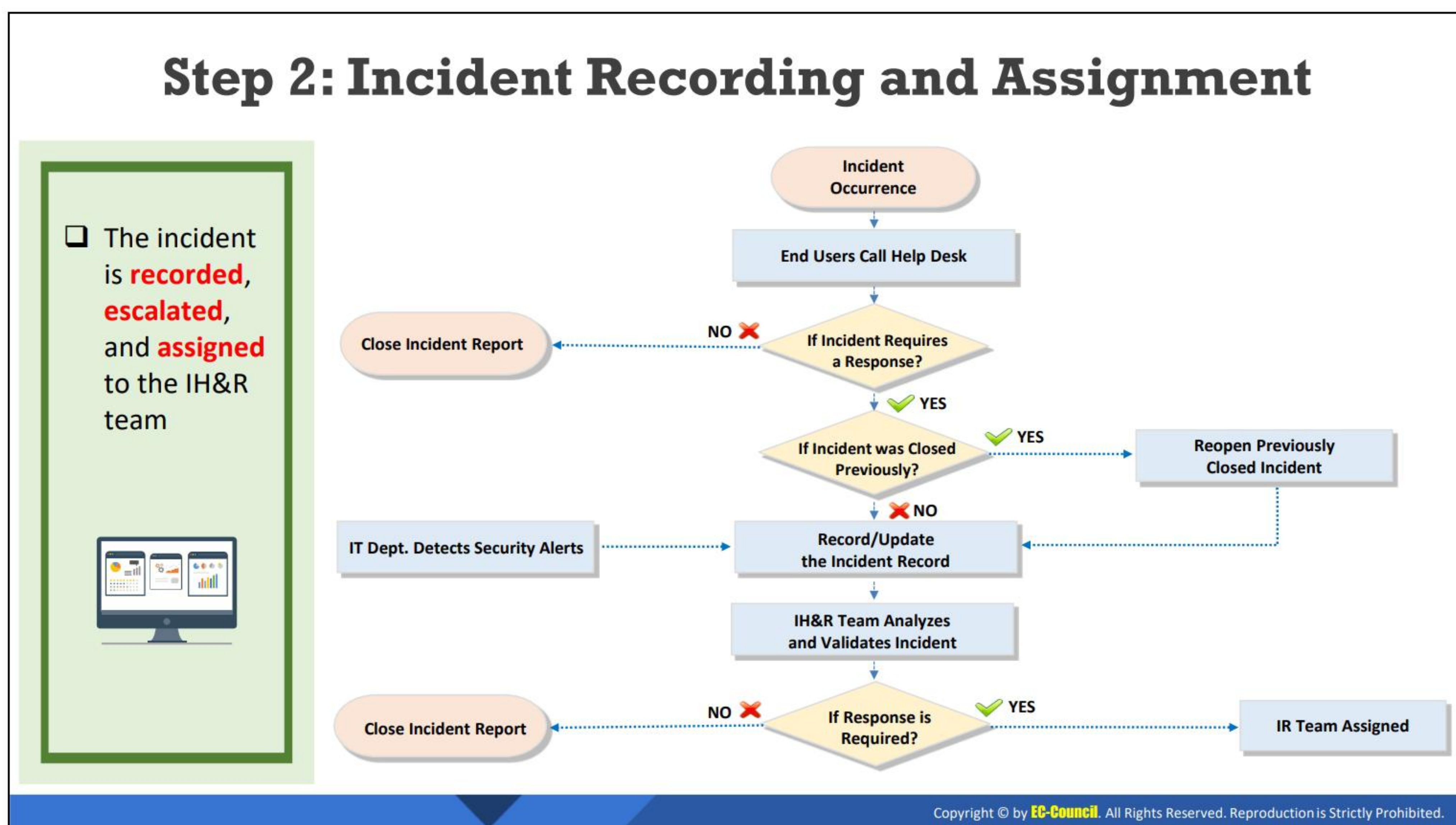
Training and Preparing IH&R Personnel

An IR team must always be completely trained and fully ready to implement an effective IR plan to protect an organization's assets and data from all types of incidents.

An organization can help the IH&R team be ready by ensuring the following:

- Availability of appropriate books, articles, magazines, whitepapers, and other technical references to improve the team's technical knowledge of the subject.
- Assignment of a part of the budget to send IH&R team members to conferences and training sessions to maintain, enhance, and increase proficiency in technical areas and security disciplines, including the legal aspects of the IR by the legal experts.
- Provision of opportunities to team members to perform other tasks associated with IR, such as preparing educational materials, conducting security awareness workshops, and conducting research.
- Consideration of the rotation of IH&R team members with other staff to achieve full coverage and to help them learn new skills.
- Maintenance of required staffing so team members can take time off.
- Creation of a mentoring program so that senior technical staff members can train less experienced staff.
- Hiring of outside experts with good technical knowledge to train IH&R team members.
- Development of various scenarios about incident handling and the institution of group discussions on various ways of handling them.

- Rigorous IH&R training for all IH&R team members, including incident responders and management.
- Incident handling mock drills to improve the performance of incident handlers, identify issues with policies and procedures, and improve communication.
- Teaching of additional skills to the team such as teamwork, communication, aptitude, effective speaking, and effective writing to help team members explain scenarios to other non-technical authorities and work groups.



Step 2: Incident Recording and Assignment

After preparation, the next step in the IH&R process is incident recording and assignment. In an organization, the incident is recorded by IT support personnel who raise an appropriate ticket after a user or employee finds an abnormal change or indicators of an incident on his/her system.

At times, incidents are recorded through Security Information and Event Management (SIEM), IDS, antivirus, and integrity checking software, among others. However, there are certain incidents that are recorded because they are clearly noticeable.

When is an incident recorded?

- Detection of anomaly in data packets sent across the network through the alarm generated by the IDS and firewall
- Antivirus alert being displayed while scanning a computer system
- System and network logs show repeated, unsuccessful login attempts.
- Data are unexpectedly corrupted or deleted.
- Unusual system crashes can indicate attacks. Attackers or intruders can damage the system that contains important data for the network.
- Audit logs show suspicious activity on the systems or network.
- System and security log files log suspicious activity either on the network or security devices.
- A staff member identifies unusual or suspicious activity on a computer system.

- A staff member identifies content on a colleague's computer that violates the organization's security policy.
- Phishing emails are received, or the company's website is defaced.
- History of activities during non-working hours shows that unauthorized access to systems has occurred.
- Social engineering attempts

When an employee of the organization finds abnormal issues pertaining to systems, network, or applications, then they immediately call IT support to inform them about the issue. IT support records the call and tries to identify the issue using the preempted questionnaire that is based on the type of incident. If IT support suspects that the issue is a security incident, then they will assign it to the IR team using a ticketing system.

The tech support or help desk personnel should analyze the event by enquiring for more details and interviewing the victim or the person who reported the incident. This will help in assessing the incident type and whether the victim had accessed some triggers accidentally.

The help desk sends all report and interview details through a ticketing system to the incident handler who assigns a first responder from the IH&R team members for analysis and validation. The first responder also analyzes the compromised systems, network, databases, and other devices to validate the incident. This helps identify the compromised systems, applications, services, and devices. The first responder lists the compromised elements and updates the incident handler about all incident details through the same ticketing system.

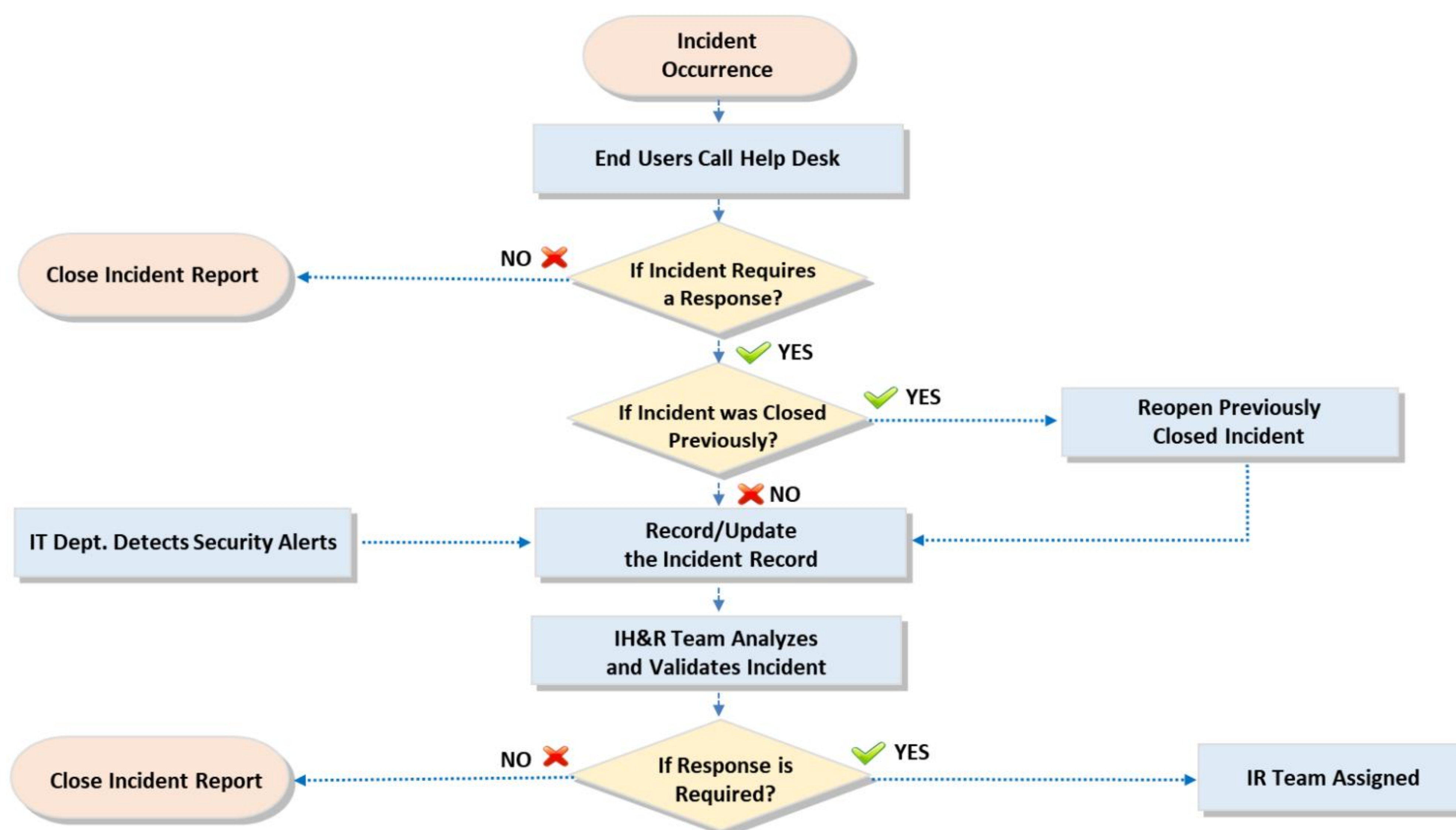
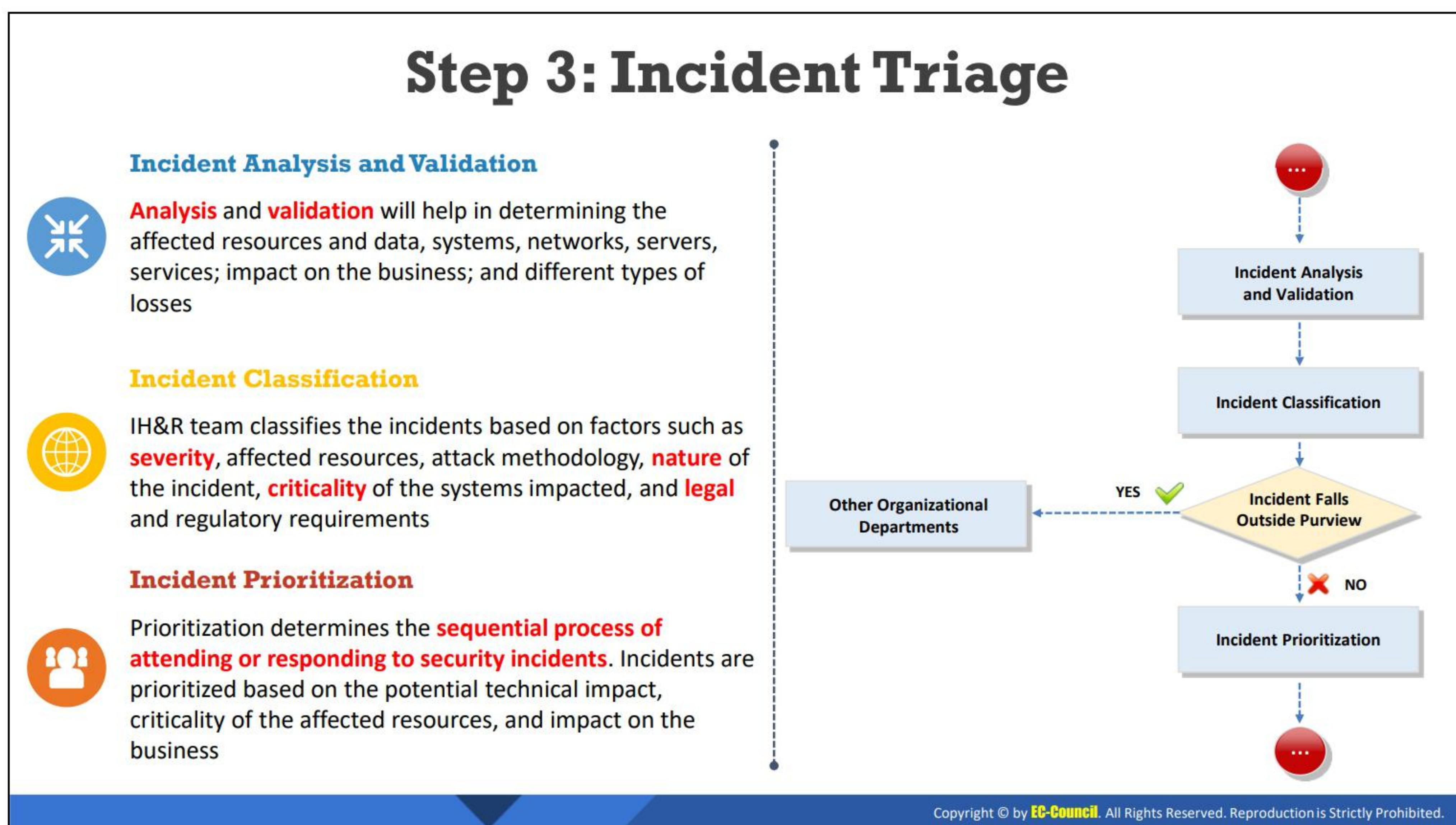


Figure 19.3: Process flow of incident recording and assignment

The tech support or help desk personnel try to determine whether the incident is the reflection of any previous incidents and conduct further examination. If it is found to be a previous

incident, then they reopen the previously closed incident to update in the IR. Otherwise, they create a record by collecting information about the incident such as security alerts and indicators from the IT department. This incident record is sent to the IR department to analyze and validate the incident. If they find the incident to be validated, then they immediately assign the IH&R team for further analysis.

The IH&R team is responsible for taking over and analyzing the incident with fine sense of judgement making and critical reasoning. The IH&R team should have a structured approach to efficiently respond to an incident. The IR team manager should classify and prioritize the incidents based on the level (high, medium, or low). The team should classify and attend to the high-priority incidents first, followed by medium- and low-priority incidents, respectively.



Step 3: Incident Triage

After incident recording and IH&R team assignment, an IH&R team is responsible for taking over and analyzing the incident with critical reasoning and good judgment. The incident triage consists of three steps: incident analysis and validation, incident classification, and incident prioritization. IH&R team will first assess the incident details and correlate the indicators with logs and other system files to validate the incident and determine the impacted systems, networks, devices, and applications. They then classify the incident depending on the type of incident. Some of the classification methods include comparing the standard criteria such as networks performance, system behavior, logs, event correlation, data packets, network traffic, files, and applications before and after the incident. Depending on the impacted resources or source of compromise or tools used to attack, the IH&R team also classifies the incident into types such as endpoint, network, malware, application, and browser incidents. Then the IH&R team manager prioritizes the incidents based on the level (high, medium, or low). The team attends to the high-priority incidents first, followed by medium- and low-priority incidents, respectively. The prioritization depends on the severity of impact and its effect on the business. Other factors that impact classification include the nature of the incident, criticality of the systems impacted, the number of systems impacted, as well as legal and regulatory requirements. If the incident falls outside the IH&R team's purview, the IH&R team contacts other organizational departments. The complete process flow of the incident triage is displayed in the following figure.

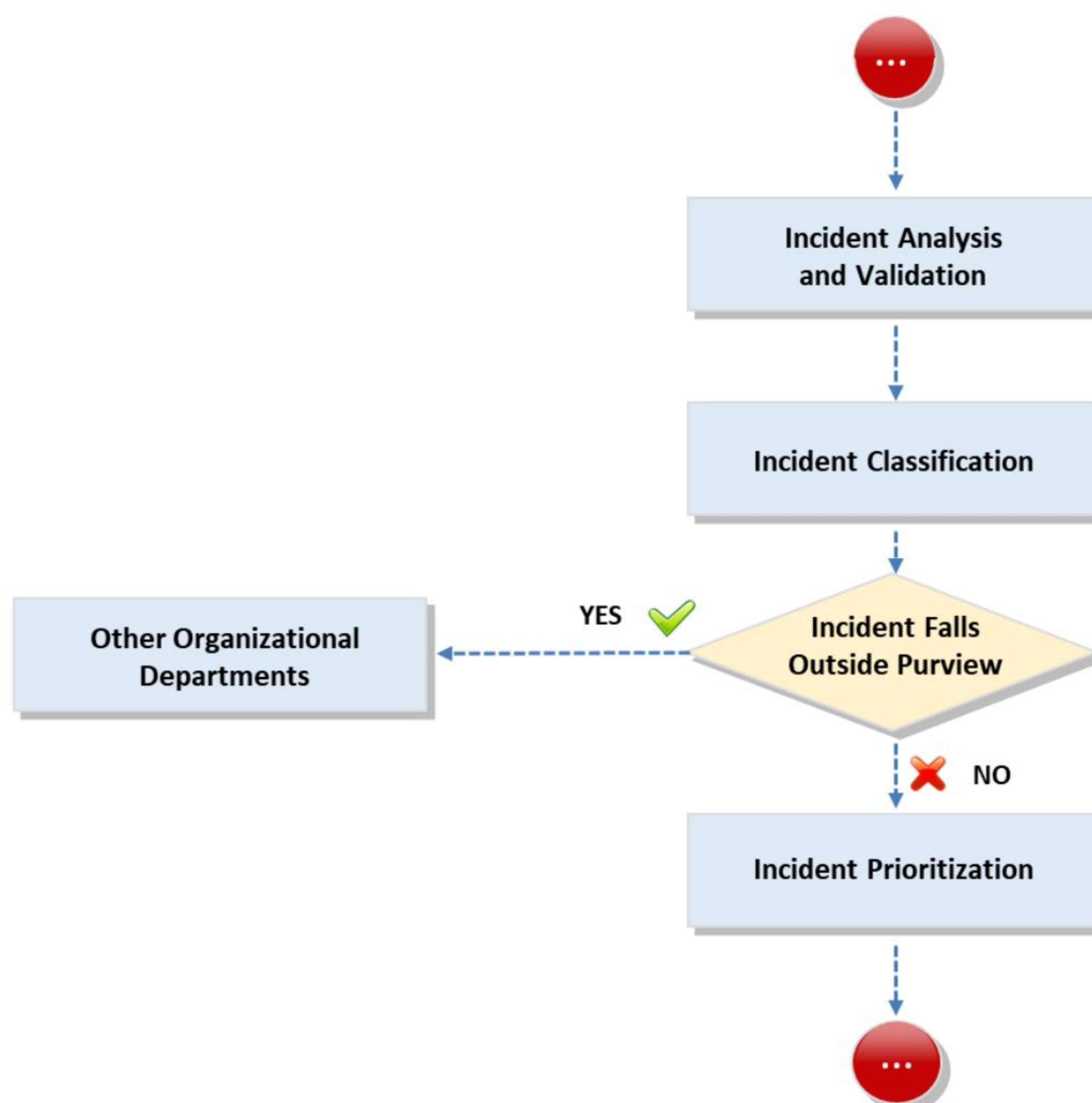


Figure 19.4: Process flow for incident triage

Incident Analysis and Validation

Incident responders need to analyze the indicators of a reported issue to verify if it is an information security incident or an error in the hardware or software components. The IH&R team should ideally evaluate each indication to determine if it is legitimate. They must find the different sources of indicators, examine the security solutions, verify the system and device logs, and identify the incident and its vectors. Even if an indication is accurate, it does not necessarily mean that an incident has occurred. All incidents cannot be security incidents; some incidents such as web server crash and modification of sensitive files could result from human errors. The incident analysis will help determine if the IH&R team needs to handle the incident, register the issue and take no further action, or pass it to other teams for processing.

The IH&R team must perform various validation activities to determine the attack details such as type, vectors, duration, source, and evidence. Analysis and validation will help determine the affected resources and data, systems, networks, servers, services; impact on the business; and different types of losses. The IH&R team can use this data to classify and prioritize the incidents.

Incident Classification

The classification of an incident depends on the potential targets and the severity of its impact. The purpose of incident classification is to gather all required information to determine its category, time required for resolving, and other criteria.

The role played by the IH&R team and their activities in this stage are as follows:

- The IH&R team evaluates the incident details and correlates them with indicators.
- The IH&R team classifies the incidents based on their severity, affected resources, and attack methodology.

Classifying the information security incident depends on several factors, including the following:

- Nature of the incident
- Criticality of the systems impacted
- Number of systems impacted
- Legal and regulatory requirements
- If the incident falls outside the IH&R team's purview, the IH&R team contacts other organizational departments.

The advantages of an effective incident classification are as follows:

- Every incident is correctly forwarded to the respective department.
- Enhances response times as the incidents are routed to the respective department
- Aids in the development of an effective knowledge base
- Increased customer satisfaction

Incident Prioritization

Prioritization of the incident is the most critical decision in the IR process as incidents must not be responded to on a first-come, first-served basis. Incident prioritization determines the sequential process of attending or responding to security incidents. The IH&R team needs to prioritize the incidents with the highest business impact so that the organization can continue to offer business services with minimal financial losses. The prioritization must depend on the severity of impact, importance of the compromised resources, disrupted operations, and losses incurred due to the incident. The incident responder is responsible for prioritizing the compromised elements and sorting them according to the most important devices or applications required for business continuity. The incident responder then assigns a team to respond to the incident by evaluating the impact and suggesting methods of detection and containment.

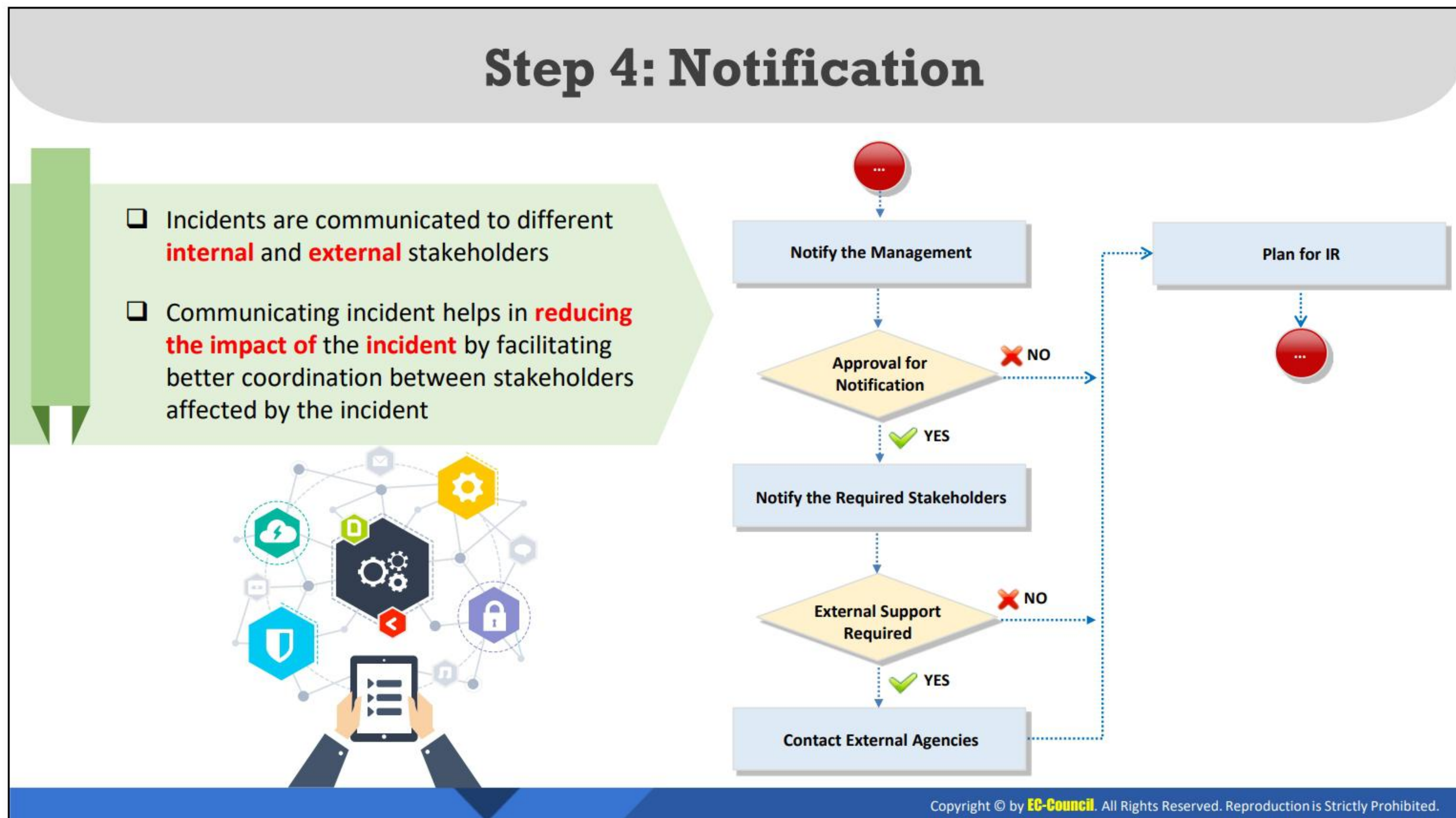
Prioritization will also help the incident responder manage the available IR staff and resources. The incident responder assigns the level of priority, predefined criteria and requirement, and urgency in restoring the compromised resource. Working on the most severe incidents will also help the organization minimize business disruption and help reduce financial and reputational loss. It can also reduce the amount and time spent on IR functions such as containment, eradication, and recovery. It will help in scheduling the tasks and increasing the ease of the process of reporting the status to stakeholders and customers.

With the emerging number of diverse cyber security incidents, assigning a category to an incident has become an essential step of the incident management process in order to prioritize the incident. Once the incident is identified in an organization, the incident responder will categorize it. Organizations adopt a common set of terminology and categorize the incidents to clearly communicate security incidents and events across different departments in an organization or to members of an IH&R team. Incident categorization enables the team to prioritize the incidents and focus on the incidents that require more attention.

The IH&R team should consider two basic elements in prioritizing incidents.

1. **Impact:** Offer an account of how severe an incident can be for the organization. It is measured in terms of the number of systems impacted by the incident, which increases the number of idle employees and, in turn, directly affects the organizational productivity.
2. **Urgency:** Usually defined in terms of the service level agreement (SLA). If an incident is raised within an organization, it should be resolved at the earliest opportunity.

The importance of impact and urgency vary across organizations. However, generally, both impact and urgency have three levels, namely, high, medium, and low.



Step 4: Notification

Communication plays a major role in swiftly responding to an incident. It helps in reducing the impact of the incident by facilitating better coordination between different stakeholders affected by the security incident. Communicate the IR process and results to the IH&R team members, so that they can understand the type of response and their responsibilities when responding to the incident. The detailed process flow of notification is displayed in the below figure:

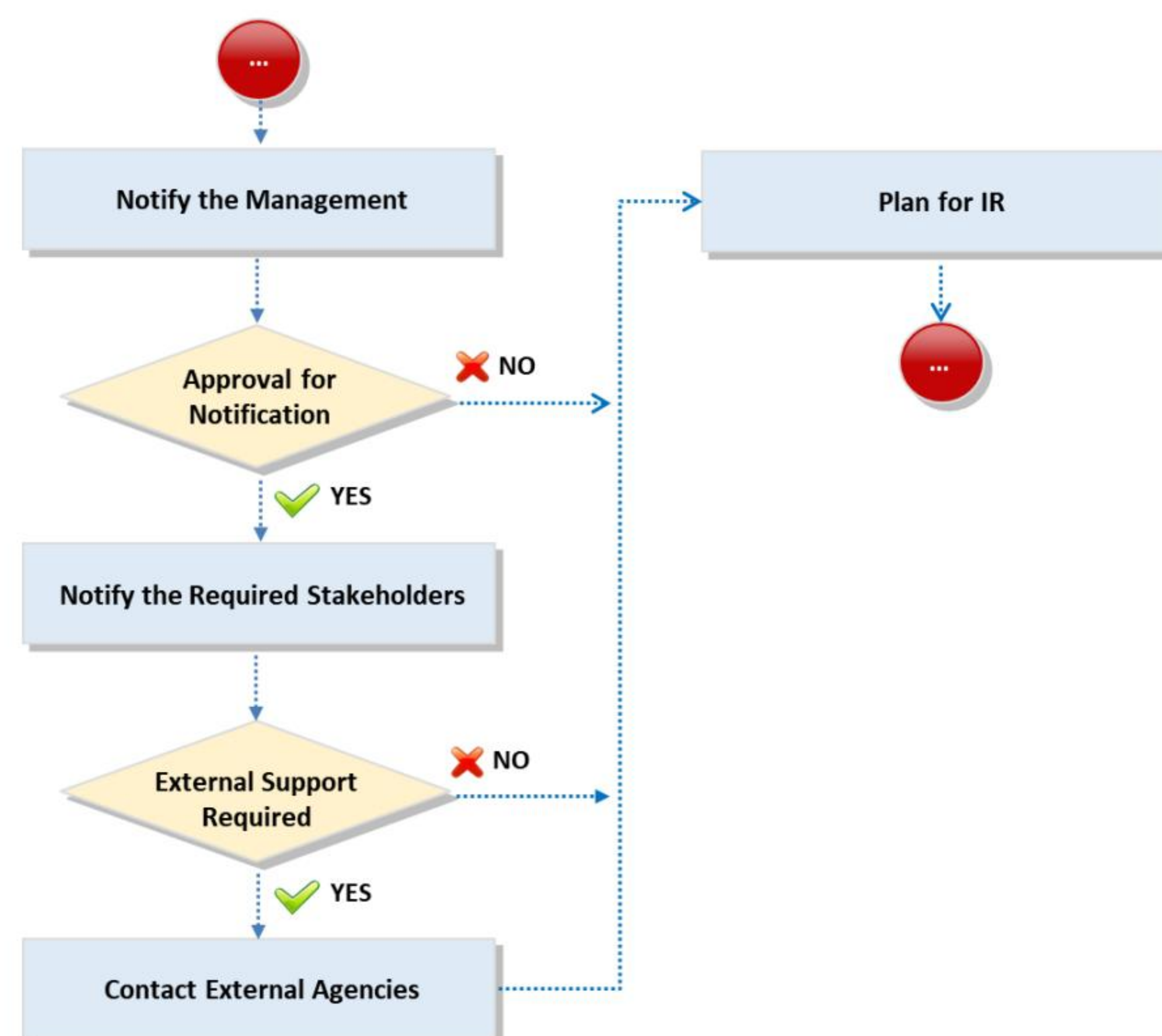


Figure 19.5: Process flow of notification

Incident responders must communicate about the severity of the incident with the management or authorized persons to gather relevant approvals for performing IR procedures. The communication would include the first report, initial processes performed to assess the situation, detection methods applied, impacted resources, and management strategy. The IH&R team should discuss the incident with a legal representative to file a lawsuit against the perpetrators.

After obtaining the approval, the IH&R team will communicate the relevant matters about the incident with the necessary stakeholders. All employees and other stakeholders must communicate with the IH&R team whenever they suspect a security breach. The IH&R team lead should discuss the breach with core team members and other members of the organization to respond to the incident effectively.

Incident responders can communicate a part of the situation to an external party after approvals from management if they need external support for responding to the incident.

After controlling and mitigating the incident, the IH&R team can disseminate the details of the incident and lessons learned in the organization and media to create awareness. Depending on the circumstances of the incident, the goal of the response strategy is to examine the most appropriate response procedure. The response plan should consider the political, technical, legal, and business factors of the incident. A response strategy generally depends on the circumstances of the incident.

The factors that affect the resources required to investigate an incident include the following:

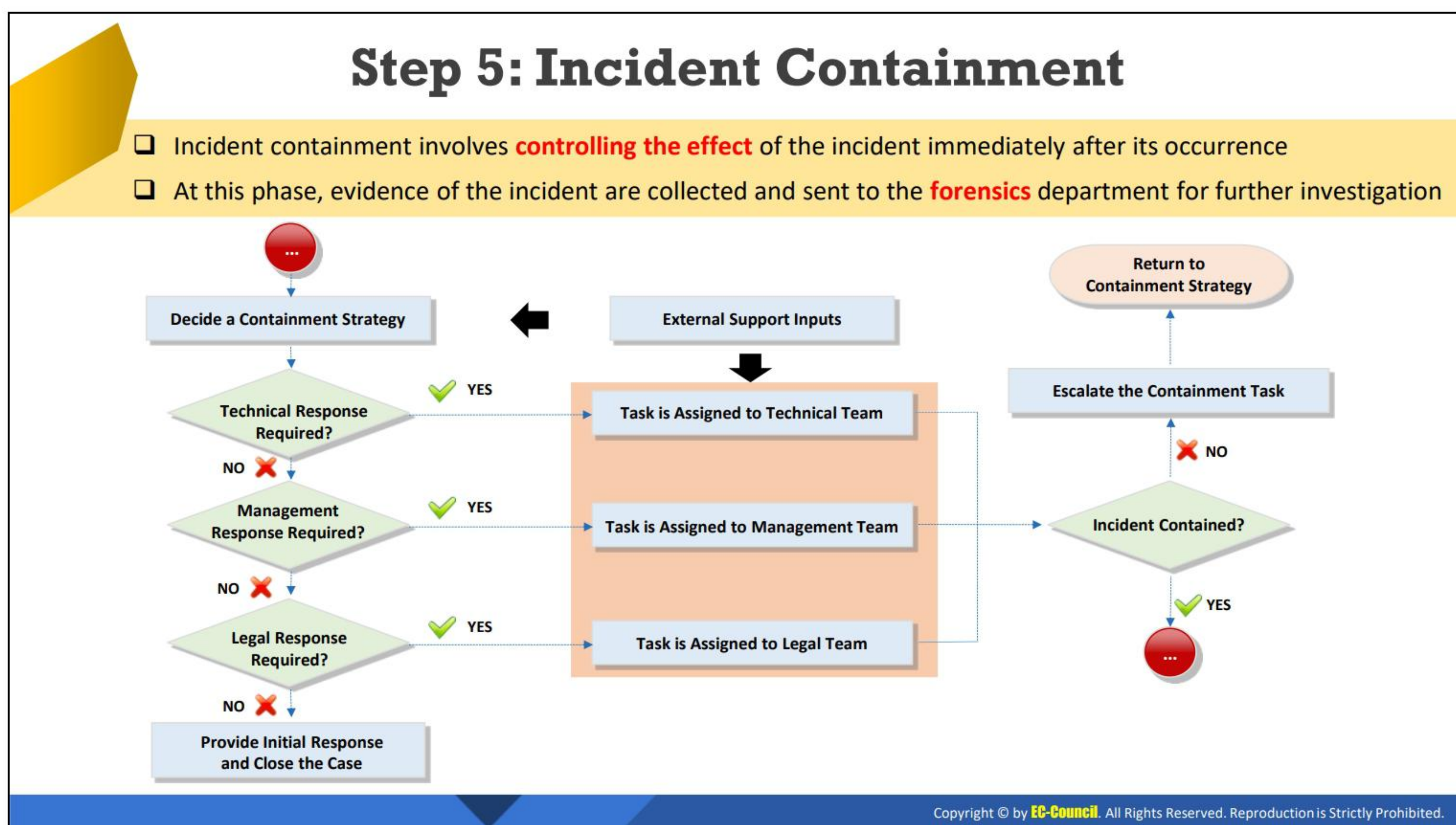
- Forensic duplication of the related computer systems
- Criminal referral
- Civil litigation
- Other aspects
 - What is the range of impact of the incident on systems?
 - How sensitive is the compromised or stolen information?
 - Who are the attackers?
 - Is the public aware of the incident?
 - What unauthorized access level have the attackers gained?
 - What skills do the attackers have?
 - What is the total downtime for the system and the user?
 - What is the total loss in dollars?

The information gathered during the initial response is important for selecting a response strategy. Before selecting the response strategy, reinvestigate the details of the incident.

An organization that is suffering from a security incident needs to notify the appropriate internal and external IH&R team to minimize any repercussions of the security event.

The IH&R team's role in the notification and planning includes the following.

- **Notifying management:** The IH&R team is responsible for notifying the management about the incident that occurred. The management should also be informed about the effects of the incident.
- **Communicating the incident:** Before communicating any information about the incident, the IH&R team should obtain documented approval from the management. The incident information should not be hidden from the stakeholders and other people. People that are likely to be affected by the incident need to be informed about the incident.
- **Disclosing the details of the incident:** Apart from broadcasting about the incident, the IH&R team should also seek approval for disclosing the details of the incident. Disclosing the details of an incident is important, as certain stakeholders of the organization need to be aware of these details.
- **Approval denied:** If the management does not provide their approval for disclosing the incident details, the IH&R team should proceed with the procedure of IR.
- **External support:** Before proceeding with an in-depth investigation of the incident, the IH&R team checks if external support is required to handle the case.
- **External support required:** If external support is required, the IH&R team contacts external agencies for input.
- **IH&R team and external support:** Once the external support joins the investigation of the incident, the IH&R team and the management team proceed with handling the incident and the response plan.



Step 5: Incident Containment

Containment focuses on limiting the scope and extent of an incident. The IH&R team plays a significant role in reducing an incident's magnitude or complexity in preventing further damage to the organization. Containment focuses on limiting the scope and extent of an incident. The aim of the containment stage is to reduce any losses and/or damages from the attacks by mitigating vulnerabilities. If the systems, networks, or workstations are compromised by a security incident, the IH&R team must determine whether to shut down the system, disconnect the network, or continue with operations in order to monitor the system's activities. The response to all these situations depends on the type and magnitude of the incident.

Common techniques used in the containment phase are as follows.

- **Disabling of specific system services**
 - Disable system services temporarily in order to reduce the impact of the incident and to continue system operations.
 - When an unknown vulnerability affects a computer, it is removed from the network until the problem is rectified.
 - Change the passwords, and disable the account.
 - Change passwords on all systems that interact with the affected system, so that there are no more infections.
- **Complete backups of the infected system**
 - Back up data on the affected systems to reduce the damage during IR. Use a system backup for further investigation of the incident.

- **Temporary shutdown of the compromised system**
 - If the compromised computer systems have no alternate options to handle the situation, then shut them down temporarily. This shutdown limits the damage caused by the incident and provides extra time to analyze the problem.
- **System restoration**
 - Replace the recovered computers with a trusted and clean backup copy.
 - Identify the incident sources such as vulnerabilities, threats, and access paths, and patch everything before restoring the system.
- **Maintaining a low profile**
 - When detecting network-based attacks, be careful to not tip off the intruder. This is because the intruder might do more harm to other systems in the network and/or erase everything they can to eliminate the chances of being traced. Maintain standard procedures, including continuing to use the IDS and the latest antivirus and anti-spam software.

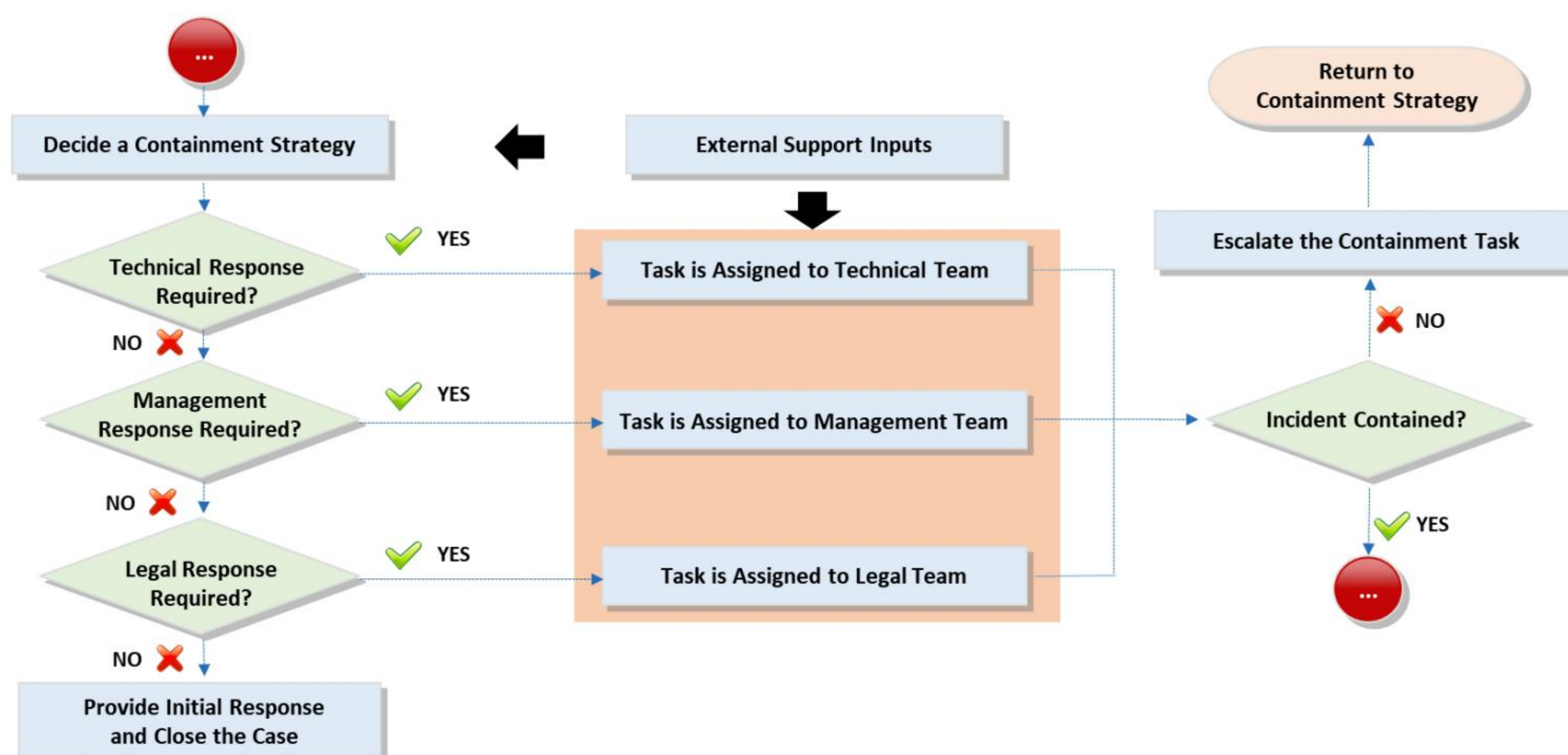


Figure 19.6: Process flow of incident containment



Guidelines for Incident Containment

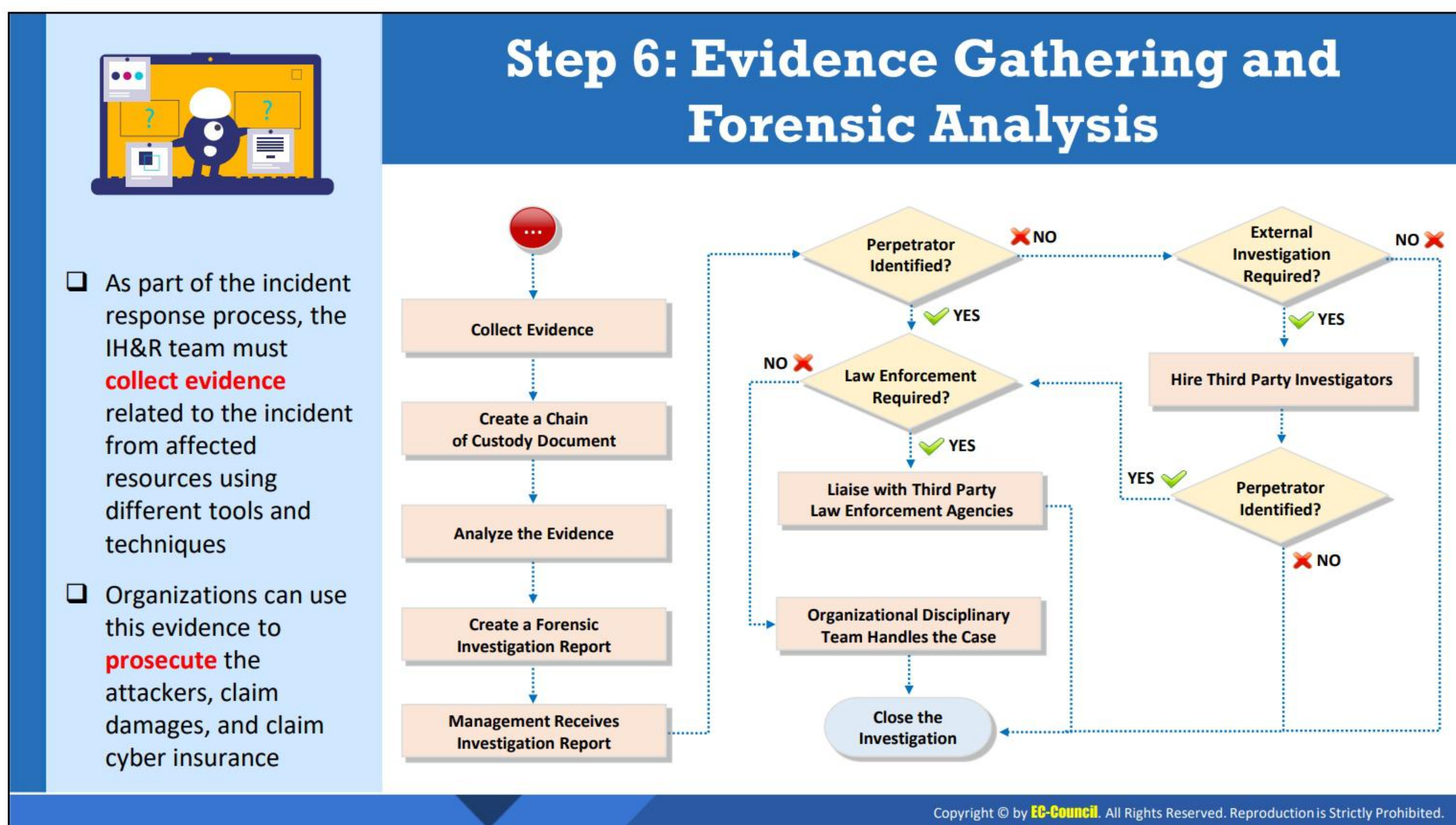
The main purpose of the containment strategy is to control the effects of the attack and restore the information system to its normal state. This is vital to ensure the organization's business continuity. A few key considerations for an IH&R team in this crucial stage are as follows.

- **Compromised code:** Compromised code can lead to a data breach, increasing the chances of an intrusion. It is important for the IH&R team to be cautious while working with the compromised code. A minor mistake can lead to code replication and can further affect the organizations' network and functioning.
- **Safe storage:** Data should be stored in a safe location so that any intrusion or external threat does not affect or alter it.
- **Acquiring logs:** The IH&R team must actively acquire and retrieve all system and router logs before, during, and after the time of occurrence of the incident. This will help the team analyze the changes the network or system underwent that caused the incident to occur.
- **Identifying risk factors:** It is important to identify the various risks if operations are to be continued.
- **Informing administrators and system owners:** The IH&R team should keep the administrators and system owners updated about the latest security threats that can affect the system. This helps implement preventive measures, avoiding the occurrence of a major incident.
- **Strong password policy:** After the IR is successfully completed, users must change their passwords. Administrators must implement a strong password policy in the organization.

- **Maintaining records:** It is important to maintain records of every action performed by the user or the system owners. Auditing and monitoring must be performed by administrators on a timely basis.

Organizations face a lot of problems when incident containment guidelines are not in place. For example, if an organization that is not well-prepared gets infected and then attacked by malware, it cannot handle the situation as effectively as an organization that follows incident containment guidelines. At times, this lack of preparedness allows malware to spread like wildfire. In these cases, people act haphazardly to find solutions for such incidents, and none of them have any ideas about how to deal with it. This delay in finding a solution can bring an organization's network, information systems, business, and reputation to the ground. Without proper guidelines in place, network administrators implement stopgap actions, trying everything they can to find the appropriate solution. This can cost the organization vast amounts of money and time. This situation can be avoided if an organization follows certain guidelines.

- **Dedicated team:** A team containing technical experts must be dedicated to handle any type of security issue. This team acts as the first responder during the time of an incident.
- **Securing the affected area:** In order to avoid any new changes being affected, the affected area must be secured. Review the information at the beginning of the identification phase.
- **Installation of honeypots:** Honeypots are invisible traps that play a vital role in enhancing security. Implementing honeypots in the network will help network defenders trap the attacker.
- **Following standard procedures:** Documented procedures are required, which the management, the IH&R TEAM, and administrators must follow.



Step 6: Evidence Gathering and Forensic Analysis

After containing an incident, an IH&R team must concentrate on digging deep into the incident by gathering more information about it, identifying its root cause, uncovering threat actors behind it, and specifying its threat vectors. These objectives can be achieved in the evidence gathering and forensic analysis phase of the IH&R process.

An IH&R team will collect crucial evidence about the incident and simultaneously create a chain of custody document. After collection and protection, investigators must analyze existing evidence to identify the cause and nature of the incident and trace the perpetrators of the crime. Moreover, they must also document the results of forensic analysis and submit them to management for further processing. If the analysis can identify the perpetrator, then the management will decide whether they will legally prosecute the perpetrator or let the organization's disciplinary team handle the case. If there is need for law enforcement, then management or a designated authority will contact a third-party law enforcement agency.

If the investigation fails to identify the perpetrator, then management must decide whether to close the investigation or to pass it to an external investigation agency for further investigation. If third-party investigators can investigate the incident and identify the perpetrator, then they will report such findings to management and management will make further decisions. Meanwhile, if third-party investigators also fail to identify the perpetrator, then the IH&R team or management can recommend an update to the IH&R processes that will enable them to carry out more successful investigations in the future.

The process flow of evidence gathering and forensics is displayed in the below figure.

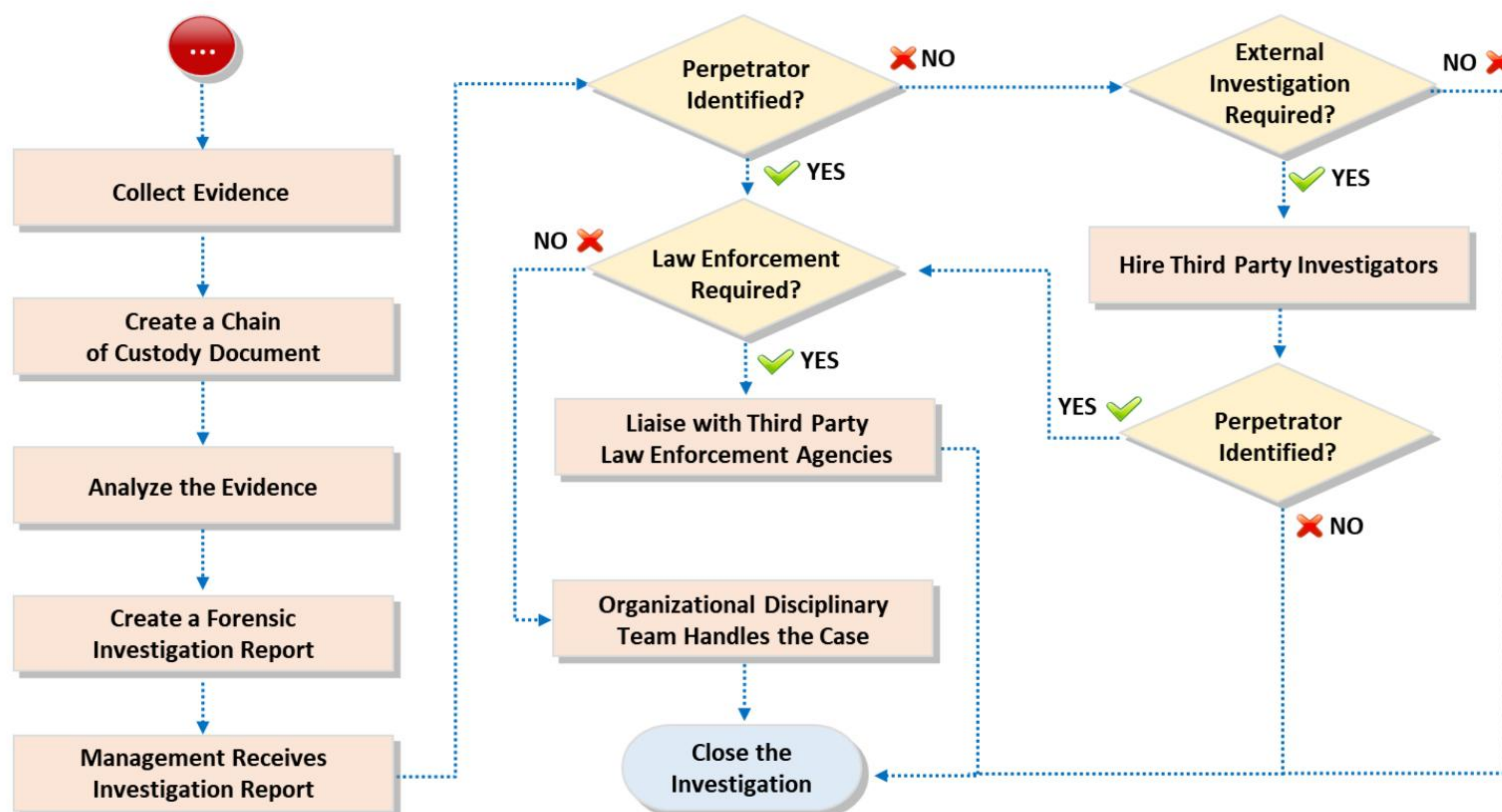
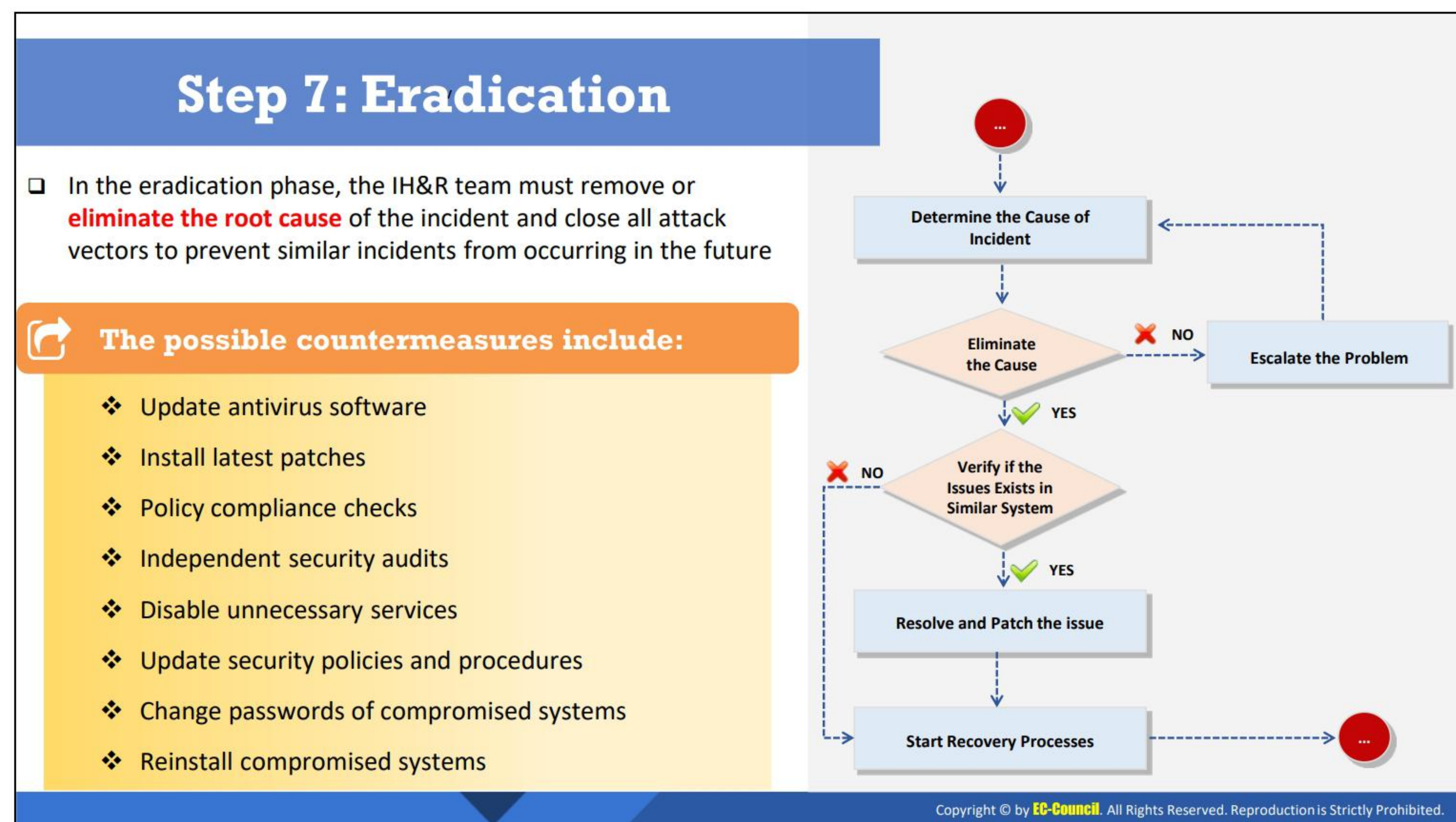


Figure 19.7: Process flow of evidence gathering and forensic analysis

More specifically, the IR team must gather evidence from victim resources using different tools and techniques and use it to eradicate the incident, create reports about the attack, and close the exploited vulnerabilities. The organization can then use this information to prosecute the attacker(s) and claim damages and cyber insurance. To be sure, evidence helps the organization find and patch any vulnerabilities exploited and other attack vectors.

- To gather evidence effectively, the organization must:
 - Train employees in first responder services
 - Create and implement forensic readiness policies and procedures
 - Enable logs on all network devices and security systems
- The process of collecting evidence includes:
 - Identification of target resources, networks, and connected resources
 - Securing and documenting the crime scene
 - Extracting fragile and volatile evidence
 - Secure handling, packaging, and transportation of the evidence devices
 - Extracting static evidence stored as media and other resources



Step 7: Eradication

After evidence gathering and forensic analysis, the IH&R team is responsible for completely eradicating the incident and its related causes, identified vulnerabilities, and so on. In the eradication phase, the IH&R team must remove or eliminate the root cause of the incident and close all attack vectors to prevent similar incidents from occurring in the future. The IH&R team must alert all service providers, developers, and manufacturers about the affected resource; check if the issue persists in similar resources across the organization; eliminate the issue from any such resources; and test whether the issue has been resolved before initiating the recovery process.

The following countermeasures will help the IH&R team eradicate the incidents:

- Update the antivirus software with new malware signature and patterns.
- Install latest patches on systems and network devices.
- Conduct independent security audits.
- Check for policy compliance and update obsolete policies and procedures.
- Disable any unnecessary services.
- Change the passwords of all compromised systems, accounts, and network devices.
- Eliminate the access paths and exploits.
- Install updated operating systems, software, and services in compromised systems only after removing traces of attack.
- Rebuild the affected or compromised systems, servers, databases, and networks.
- Validate the effectiveness of all corrective steps or countermeasures.

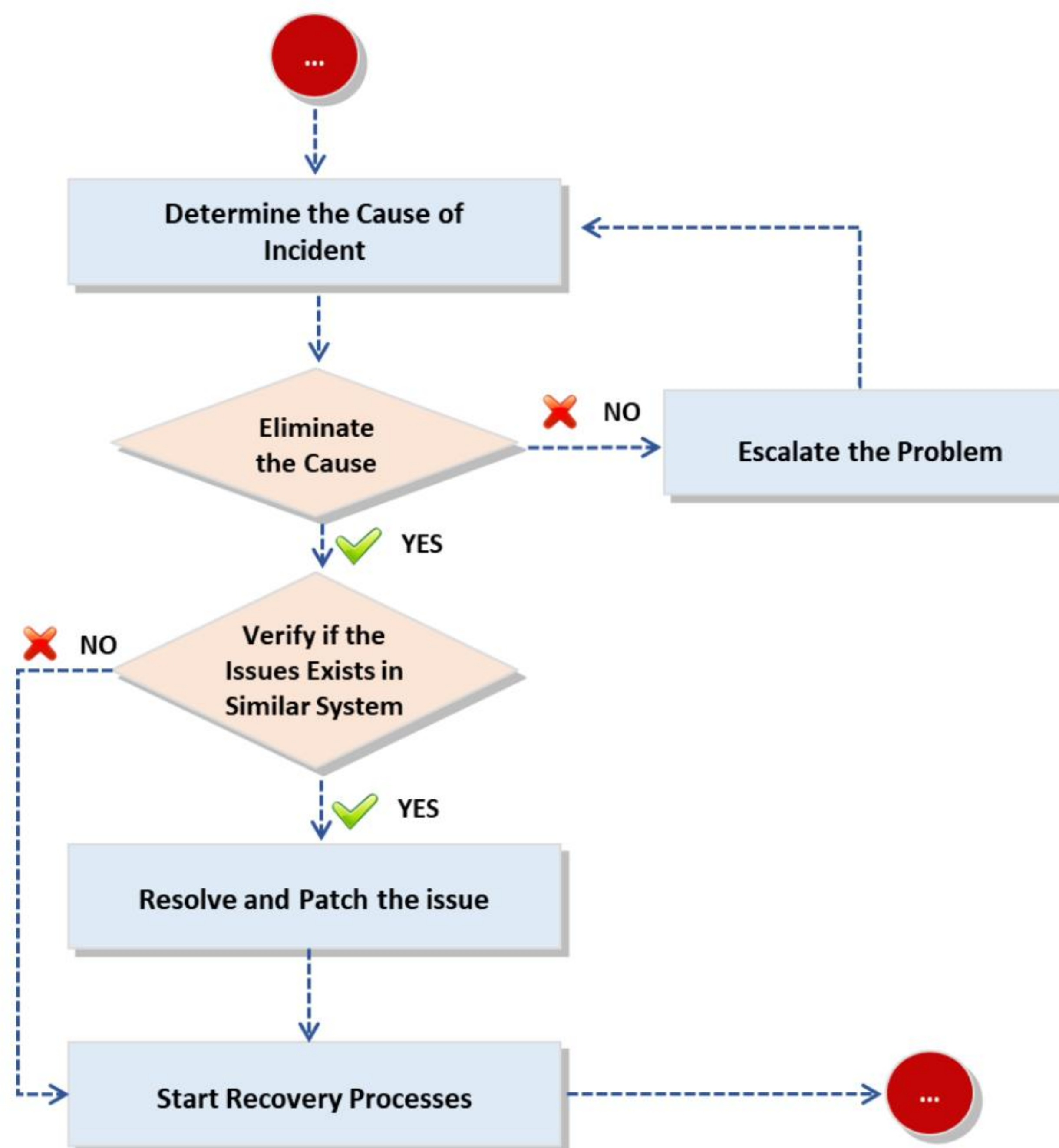


Figure 19.8: Process flow of eradication



Step 8: Recovery

After eliminating the cause of the incident from all systems and resources, an IH&R team has to identify whether the data is lost. If the data is lost, then the IH&R team has to recover the data from backups and restart the affected services and processes in order to maintain business continuity.

Recovery is the process of restoring lost data from backup media. During this process, an IH&R team has to make sure the backup does not have traces of malware or attack vectors before performing the restore. The time it takes to recover a system generally depends on the extent of the security breach. Recovery involves various techniques such as network perimeter security, strengthening user ID credentials, effective patch management, renewing files and software, and rebuilding systems. After recovering all lost data, the IH&R team must restart all the withheld processes and services.

Recovering a system after an incident generally depends on the extent of the security breach. An IH&R team should decide whether to restore the existing system or completely rebuild the system—notably, the team can use the system backup for either process.

Therefore, the two steps in systems recovery are:

- **Determine the Course of Action**

Devise various strategies for system recovery according to the impact of the incident and select an appropriate plan after considering the availability of resources, the criticality of affected systems, and the results of a cost-benefit analysis.

- **Monitor and Validate the Systems**

By monitoring and validating affected systems, the IH&R team can ensure that recovered systems do not have any traces of incident causes and are operating within normal conditions. Helpful to note here for our purposes is that validation also involves checking the integrity of restored information from a backup. Teams should also be sure to conduct regular vulnerability assessments and penetration testing to monitor system behavior and possible vulnerabilities in the system or network. To be sure, it is important to monitor the system for potential back doors, which can result in the loss of data.

Notable actions the response team must perform during the recovery stage include:

- Rebuilding the system by installing a new OS
- Restoring user data from trusted backups
- Examining protection and detection methods
- Examining security patches before installation and enabling system logging

The IR team must also determine the integrity of the backup file by reading its data and verifying its integrity before restoring it on the systems. It is also important for the team to verify success of the operation and the normal condition of the system after installing the backup. The team must monitor the system using network loggers, system log files, and potential back doors after installation and during usage.

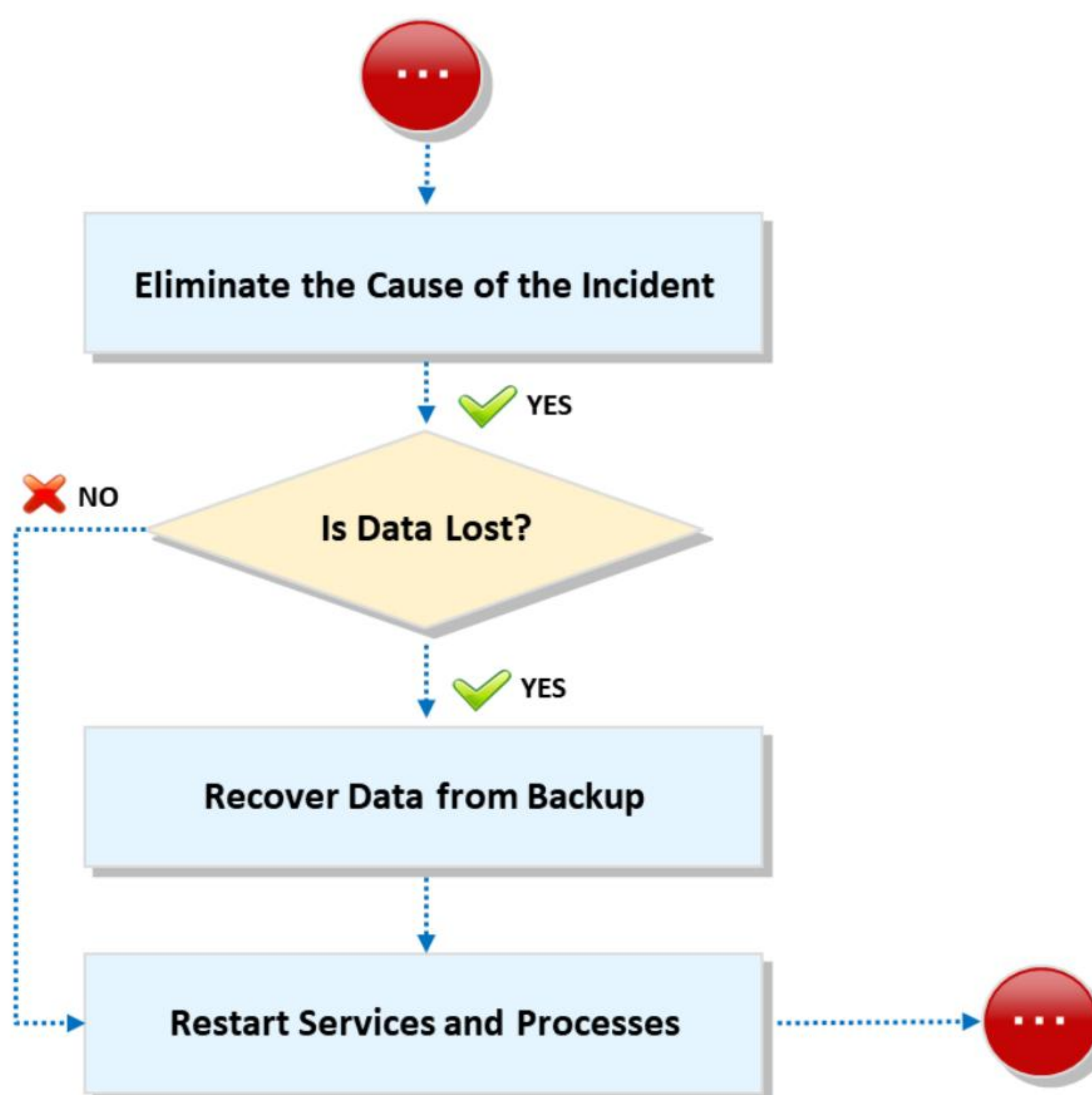


Figure 19.9: Process flow of recovery



Step 9: Post-Incident Activities

After eradicating the incident, an IH&R team must perform certain activities to improve its response to future attacks. Accordingly, “post-incident activities” refer to the actions and precautions that an organization and response team must perform to be better prepared to handle and respond to future incidents. In this stage, the team will discuss all the drawbacks it faced during the response functions and try to eliminate them.

Post-incident activities help in evaluating and improving the effectiveness of IR processes by helping responders assess lags in security postures, settings, and configurations across their organization. They also help in suggesting measures and security products an organization can use to harden its security and optimize its policies.

To be sure, organizations should conduct meetings with staff and other involved parties to understand all lessons learned from the incident and improve in any areas in which it currently falls behind. These activities will help in evaluating and improving the effectiveness of IR processes by offering insight into how to best update policies, procedures, security postures, settings, and configurations across the organization to build a robust network.

Moreover, to learn from the experience, the IH&R team must have a document about the incident that reveals any details about the incident, vulnerabilities exploited, response measures implemented, results, pitfalls in the response process, and drawbacks in communication and management. Accordingly, as noted throughout this module, the IH&R team should document every step of the IR as well as the lessons implemented. The IH&R team must then communicate any updates and new implementations to clients, customers, management, and other stakeholders.

The following figure displays the overall process flow of post-incident activities:

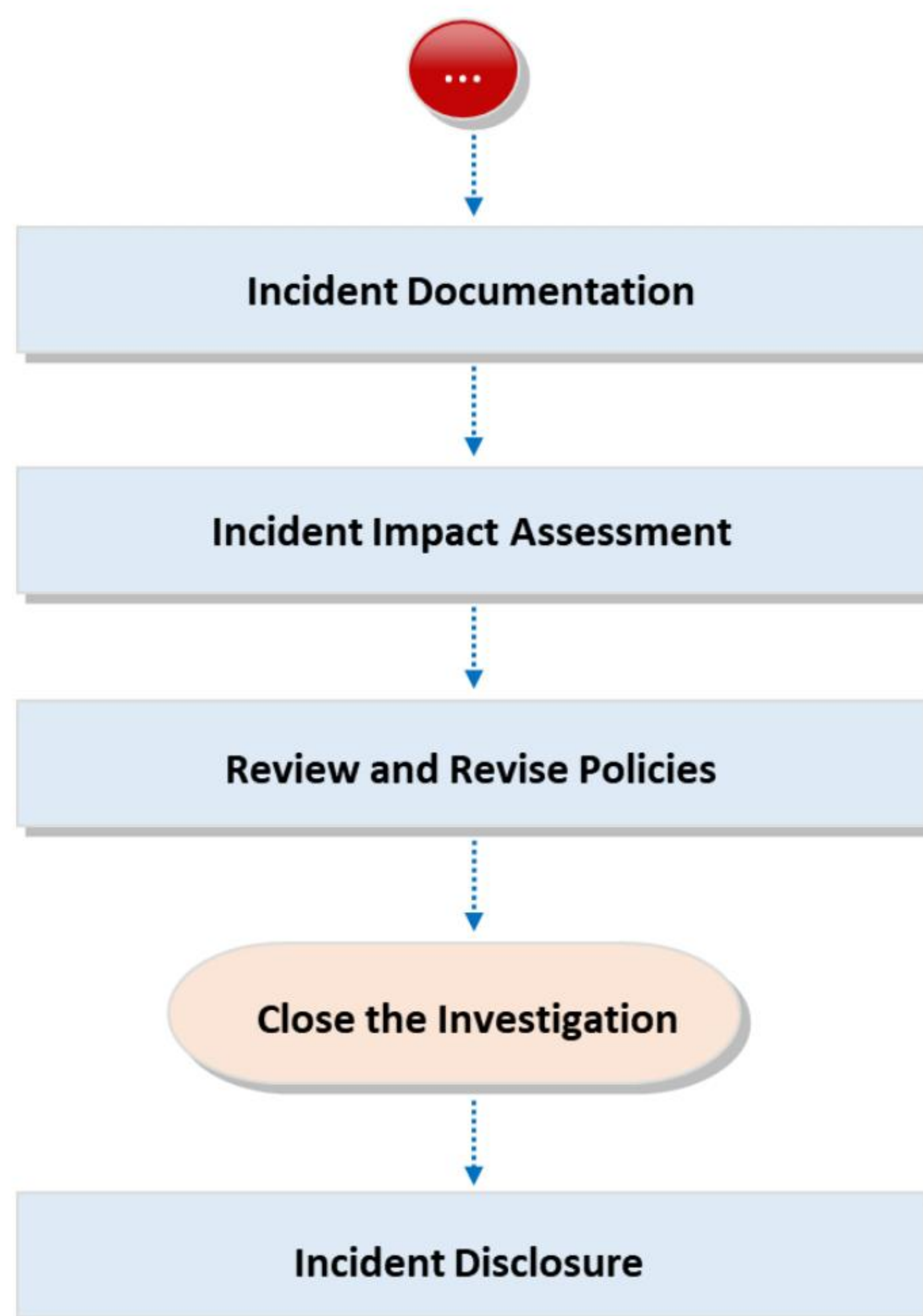


Figure 19.10: Process flow of post-incident activities

Incident Documentation

As stated above, the IH&R team should document various processes while handling and responding to an incident. The documentation should describe the security breach and detail the measures taken in response, such as who handled the incident, when the incident was handled, and the reasons behind the occurrence of the incident. The steps taken and conclusions reached should be documented immediately after the forensic process.

Incident Impact Assessment

“Incident impact assessment” refers to the process of determining all types of losses that occur due to an incident. Incident responders must find and list all affected devices, networks, applications, and software to evaluate the impact of the incident. An incident impact assessment must include details such as type of impact, method of detection, response process, and eradication measures.

Review and Revise Policies

Reviewing and revising security policies is a key step in the IH&R process that helps prevent future incidents. Helpful to note is that the review and revision of security policies is simply the implementation of the lessons learned from previous incidents.

Close the Investigation

After conducting a detailed investigation, documenting the incident, and revising relevant policies, the investigation can be officially closed; management should be informed that the investigation has closed.

Incident Disclosure

After closing the investigation, the incident disclosure takes place. An organization hit by a security incident needs to disclose the incident's details to various entities. Ultimately, at this stage an organization will decide what details to disclose to respective stakeholders. The disclosure procedure varies by company and stakeholders. An IH&R team must consult its legal department before sharing any information with external entities.

The following is a list of possible entities that may be interested in information related to such a cyber incident:

- Law Enforcement
- Regional Judiciary
- Regulatory Authorities
- Media
- Stakeholders
- Stockholders
- Breach Victims
- Vendors
- Customers
- General Public
- Third Parties
- Other CERTs/CSIRTs

Module Summary

- ☐ This module discussed the concepts of incident response
- ☐ It discussed the role of the first responder in incident response
- ☐ It also discussed the incident handling and response process
- ☐ Finally, this module provided an overview of the various phases involved in incident handling and response
- ☐ In the next module, we will discuss computer forensics in detail



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

This module discussed the concepts of incident response. It discussed the role of the first responder in incident response. It also discussed the incident handling and response process. Finally, this module provided an overview of the various phases involved in incident handling and response.

In the next module, we will discuss computer forensics in detail.