Natural Resources Canada | Ressources naturelles Canada

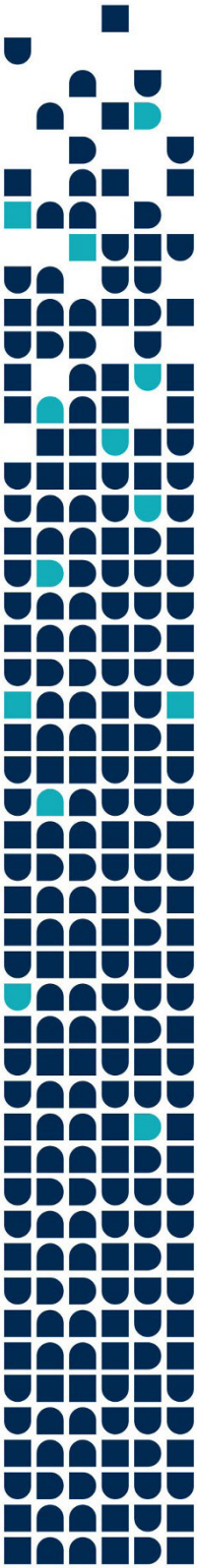
# IACS Cyber Security Incident Response Playbook

Technical guideline supported by Natural Resources Canada under the Cyber Security and Critical Infrastructure Program (CCEIP)

BBA Document No. / Rev. 6691002-000000-4S-ERA-0003 / RAA

March 2022

https://t.me/learningnets



Natural Resources Canada | Ressources naturelles Canada


Prepared by:

**Ahmad Ahmadi, PhD**
IACS Cyber Security Specialist

**James Park, P.Eng., MBA, PMP**
IACS Cyber Security Specialist

**Jonathan Ma, EIT**
IACS Cyber Security Specialist

Verified by:

**Pierre Janse van Rensburg, GCIH**
Senior Consulting Expert,
IACS Cyber Security



This Document has been prepared by BBA for its Client and may be used solely by the Client and shall not be used nor relied upon by any other party or for any other purpose without the express prior written consent of BBA. BBA accepts no responsibility for losses, claims, expenses or damages, if any, suffered by a third party as a result of any decisions made or actions based on this Document.

While it is believed that the information contained herein is reliable under the conditions and subject to the limitations set forth in the Document, this Document is based on information not within the control of BBA, nor has said information been verified by BBA, and BBA therefore cannot and does not guarantee its sufficiency and accuracy. The comments in the Document reflect BBA's best judgment in light of the information available to it at the time of preparation.

Use of this Document acknowledges acceptance of the foregoing conditions.



**https://t.me/learningnets**

# Table of Contents



**https://t.me/learningnets**

## List of Figures



## List of Tables



https://t.me/learningnets

CHAPTER 1

# Introduction

## 1.1 Scope

Canadian companies that operate critical Industrial Automation and Control Systems (IACS) need a comprehensive incident response plan to deal with cyber security incidents. If a cyber-attack compromises field control devices, it could create safety hazards that put employees and the public at risk.

This IACS Cyber Security Incident Response Playbook provides a plan that integrates various internationally recognized cyber security IT and OT incident response standards with the Incident Command System (ICS), an industry-agency proven, and internationally accepted, emergency management system. This playbook is developed to accompany the advancement of the standards, best practices, and guidelines related to cyber security in the critical infrastructure sectors. The targeted stakeholders are companies operating IACS in the following industries: Water, Energy & Utilities (Electricity, Oil, Gas), Food, and Manufacturing. The IACS Cyber Security Incident Response Playbook would be published and made available to the government, industry, and the general public.

The objectives of this IACS Cyber Security Incident Response Playbook are to ensure that an organization or company can:

- Manage its incident response safely, efficiently, and effectively.
- Promptly coordinate available resources in executing incident response tasks outside of normal operations.
- Return to normal operations in the shortest possible time while minimizing the business impact.


https://t.me/learningnets

## 1.2 The Need for Incident Response Plans

According to definitions presented in the *NIST Special Publication 800-61* [1], a *cyber security event* is any apparent activity in a computer system. For example, events could include a user authenticating to a server, a server receiving a DNP request, or a firewall blocking a web-service connection. *Adverse cyber security events* are events with negative impacts to a computer system, such as execution of malware or virus, loss of network connection, and storage drive failure.

> A *cyber security incident* is "an occurrence that results in actual or potential jeopardy to the [safety, reliability,] confidentiality, integrity or availability of the information, the system processes, stores, or transmits or that constitutes [an]…imminent threat of violation of security policies, security procedures, or acceptable use policies" [1]. IACS cyber security incident also includes compromise or potential compromise of cyber assets that may impact or disrupt the operational processes. Note that the organization's regulatory framework could have more specific definitions that relate to the organization's environment. The users of this incident playbook are advised to consult such material.

Examples of cyber security incidents include actual or suspected denial of control action, reprogramming of control devices, spoofing of system status information, manipulation of control logic, modification of safety systems, and malware on the control system. For more details about Threat Sources, Vulnerabilities, and Incidents, refer to *NIST Special Publication 800-82, Appendix C* [2].

When a cyber security incident occurs in an IACS environment, it is critical to respond promptly, effectively, and efficiently to minimize the impact on business operations, system availability, and personnel or public safety. A company will benefit significantly during an actual cyber security incident by having a well-defined incident response plan ready before the event. The incident response plan will support responding to a security incident systematically, proactively, and efficiently. The incident response plan is a continuously evolving system that can be updated based on lessons learned during an actual incident or an exercise drill.

For many Canadian companies, the development of incident response capabilities is driven purely by internal business continuity directives. However, for other companies, this may also be mandated due to various laws and regulations. Examples include:

- The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) Standards, which aim to protect the infrastructure deemed critical to the normal operation of North America's electricity grid.
- Canada's Nuclear Regulator (CNSC) Physical Design – Design of Reactor Facilities: Nuclear Power Plants (REGDOC-2.5.2), which mandates the creation of a cyber security program to protect computer-based instrumentation and control systems.
- CSA Z246.2-18, Emergency preparedness and response for petroleum and natural gas industry systems, which is a standard that defines the central concepts of emergency management – prevention / mitigation, preparedness, response, and recovery.
- CAN/CSA-ISO/IEC 27035-1, Information technology — Security techniques — Information security incident management, which covers principles of incident management as they relate to the different stages of incident response.
- CSA Z1600, Emergency and continuity management program, which defines a standard process to develop, use, and maintain such a program.

## 1.3 Incident Command System Background

The Incident Command System (ICS) is a standardized emergency management system designed to provide robust and efficient incident management by effectively coordinating facilities, equipment, personnel, procedures, and communications within an organization. It is designed to be flexible in managing both small and large emergency events.

ICS was developed initially to support inter-agency responses to wildfires in California and Arizona. The Incident Command System is now an industry-agency proven and internationally accepted emergency management system. The system is now a component of the National Incident Management System (NIMS) in the United States, managed by the Federal Emergency Management Agency (FEMA). "The Incident Command System was first implemented in Canada on a large


https://t.me/learningnets

scale by the Province of British Columbia in the mid-1990s. In 2002, the Canadian Interagency Forest Fire Centre (CIFFC), as part of its mandate to its provincial, territorial, and federal members, introduced the CIFFC ICS Canadian Version doctrine and complete set of training materials to the wildland fire community across Canada (all provincial, territorial and federal agencies responsible for wildland fire management). A number of non-wildland fire organizations also soon adopted this model, and over the ensuing years, adoption of the system increased significantly"[1].

ICS has three main objectives:

- Provide organized, standardized, and flexible division of labour.
- Ensure overall safety during incident response.
- Ensure the incident response is handled in an efficient and effective manner.

The ICS team structure is designed to be flexible to expand or shrink to meet the dynamic needs of incident management.

Section 2.3.2 of this document further explains the ICS framework.

For more detailed information regarding ICS, please refer to the FEMA IS-100 training. An Interactive Web-Based Course is available on the FEMA website.

## 1.4 Normative References

- «NIST Special Publication 800-30 - Guide for Conducting Risk Assessment,» National Institute of Standards and Technology, 2012.
- «NIST Special Publication 800-61 – Computer Security Incident Handling Guide,» National Institute of Standards and Technology, 2012.
- «NIST Special Publication 800-82– Guide to Industrial Control Systems (ICS) Security,» National Institute of Standards and Technology, 2015.
- «ISO/IEC 27005 - Information Security Risk Management,» International Organization for Standardization, 2018.
- «ISA-62433-3-2 Security Risk Assessment and System Design,» International Society of Automation, 2018.
- «ISO 31000: Risk Management - Guidelines,» International Organization for Standardization, 2018.
- «Open Risk Analysis Technical Standard (O-RA),» The Open Group, 2013.
- «ISO 31010: Risk Management - Risk Assessment Techniques,» International Organization for Standardization, 2019.
- «ICS 100 - Introduction to the Incident Command System,» FEMA Emergency Management Institute, 2018.

## 1.5 Document Structure

The remainder of this document contains the description of the cyber security incident response concepts, processes, activities, examples, and other supporting information as follows:

- **Chapter 2** describes the concept and components of the cyber security incident response within operational environments and their relationship with the Incident Command System (ICS). It describes **what** the components of IACS cyber security incident response are.
- **Chapter 3** describes the processes of cyber security incident response components mentioned in Chapter 2. It describes **how to** utilize the components in an IACS cyber security incident response process.

The following format is used to describe each activity in this chapter:

**Input:** Identifies the input values the activity needs to operate

**Action:** Describes the activity

**Output:** Identifies the activity deliverables

**Implementation guidance:**

Provides guidance to develop the action process based on the relevant incident response components.

1 https://www.icscanada.ca/en/about+ics+canada.html


https://t.me/learningnets

CHAPTER 2

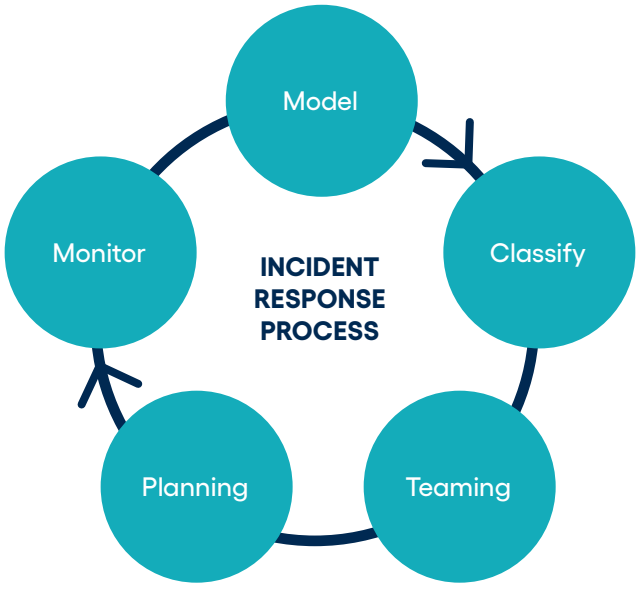
# Components of Incident Response

This chapter describes the fundamental concepts associated with managing cyber security incidents within an IACS environment. An overview of the organizational environment, the incident classification method, the Incident Command System (ICS) team structure, incident monitoring, and planning are provided.

The cyber security incident response process consists of the following components:

1. Modeling the Organizational Environment
2. Classifying Incidents
3. Forming Teams
4. Planning Responses
5. Monitoring Incidents

**Figure 1: Operational Cyber Security Incident Response Components**





https://t.me/learningnets

The first component, **Modeling the Organizational Environment**, defines the processes to model the organizational environment. This component aims to identify organizational structure and expertise, identify and classify IACS assets, identify existing cyber security controls, and monitor risks to the assets. See Section 2.1 for details.

> The second component, **Classifying Incidents**, determines how to classify cyber security incidents and the related impacts. The incident classification consists of a classification of incident types, impact analysis, and severity analysis. A pre-defined classification methodology will expedite the initial assessment of an actual incident and formulate the Cyber Security Incident Response Team (CSIRT). See Section 2.2 for details.

The third component, **Forming Teams**, is the methodology for staffing the incident response team. This is based on the Incident Command System (ICS) framework. It provides a consistent, organization-wide, command structure that can efficiently manage cyber security incidents. The purpose of this component is to determine the internal and external services that are required for the incident management process, identify the modules and resources that deliver specific task requirements, identify stakeholders and human resources with defined roles and responsibilities, define the decision and escalation path, and define the structure, responsibilities, and tools for communications among stakeholders. See Section 2.3 for details.

The fourth component, **Planning Responses**, is to establish / identify the plans before actual incidents. This component aims to define policies, objectives, and strategies, and plan the course of actions to take when a cyber incident happens. The policies, plans, and procedures should clearly define the roles, responsibilities, expectations, alert measures, and communication methodologies. See Section 2.4 for details.

The fifth component, **Monitoring Incidents**, develops a mechanism to monitor cyber security events and documentation over time. The incident monitoring component aims to identify impacting changes to the organization, business processes, operational systems, and their environments. Moreover, this component documents all events, changes, decisions, and communications and defines alert measures for all monitored elements. See Section 2.5 for details.

## 2.1 Organizational Environment

### 2.1.1 Organizational Structure

A simplified three-tier version of the organizational model presented in the *NIST-SP 800-39* [3] publication is considered in this playbook. The three management tiers are shown in Figure 2: IACS Cyber Security - Three Management Tiers – Organizational, Business Process, and Operational Systems – and represent a typical organizational structure. It is important to note that the departments and operational systems may vary between different companies.The Incident Response Process Owner is responsible for overseeing the planning, preparation, and execution of incident management activities based on the cyber security incident management policy and Incident Response Plan(s) (IRP). They define the roles and responsibilities of CSIRT members and other stakeholders. They also define the goals of incident response activities.

**Figure 2: IACS Cyber Security - Three Management Tiers**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tier 1 Organizational** | Corporate | | | | | | | | | | |
| **Tier 2 Business Process** | Security | | Operations | | | Health, Safety, and Environment | | Financial | Legal | Human Resources | ... |
| **Tier 3 Operational Systems** | IT Systems | Physical Security Systems | OT Systems | Telecommunications | SCADA | Health Systems | Safety Controls | Payroll System | Compliance Monitoring | Human Resources System | ... |


https://t.me/learningnets

- **Organizational (Tier 1):**
  The Organizational tier represents the highest level of management which oversees the operation of the entire company. Positions at this tier include corporate-level management such as CEO, CFO, the Board of Directors, and Executive Vice Presidents. Tier 1 management would likely assemble to form a separate Crisis Management Team (CMT) in response to severe cyber security incidents. The CMT manages the overall business strategies and response to incidents that may affect the company at a corporate level. For most other incidents, they would only be notified and updated of the incident status by the CSIRT.

- **Business Process (Tier 2):**
  The Business Process tier represents the middle management responsible for handling a specific business function such as Security, Human Resources, and Finance. Positions at this tier could include Vice Presidents, Department Directors, and Team Managers. The Tier 2 management's involvement in incident response would start at medium-level cyber security incidents with department-wide threats. In lower-level incidents, they would only be notified and updated of the incident status by the CSIRT.

- **Operational System (Tier 3):**
  The Operational System tier consists of teams that own and maintain the operational systems. Positions at this tier could include system-level personnel such as Team Supervisors, Team Leads, Operators, and System Administrators. Tier 3 management and personnel would actively participate in all cyber security incident responses.

#### 2.1.1.1 Inter-tier Response

This Incident Response Playbook focuses on the processes associated with IACS cyber security incident response. The initial IACS cyber security incident detection, identification, and classification would likely be conducted at Tier 3 within the Operations teams. However, the CSIRT could be formulated across the tiers depending on the severity and complexity of the incident. This concept is expanded on in Section 2.3.4. The ICS framework facilitates the operation and integration of these inter-tier response processes.

#### 2.1.1.2 Identifying Expertise

It is essential to identify different roles within an organization required for planning and implementing cyber security incident response. Depending on the incident severity and size, different levels of role segregation would be needed in the CSIRT. Following are examples of resources, expertise, and abilities that one would look for to develop a cyber incident response plan and formulate a response team.

- **Management (Tier 1, Tier 2, Tier 3)**
  Management functions can be found in all levels of the organizational tiers. The upper management (i.e., Tier 1) is generally responsible for advising or enforcing the establishment of a corporate cyber incident response policy.

  The middle management (i.e., Tier 2) is generally responsible for developing and maintaining cyber incident response policies at the corporate or business unit levels.

  Tier 3 management (i.e., supervisors, managers, and leads) is generally responsible for developing and maintaining system-level cyber incident policies, plans, and procedures. During an incident, they would likely be responsible for managing all incident response activities, including initial incident classification and the formulation of CSIRT.

- **IACS Support (Tier 2, Tier 3)**
  IACS Support consists of IACS / OT technical experts such as system administrators, network administrators, and cyber security specialists. The IACS Support personnel would likely conduct the initial IACS cyber security incident detection, identification, and classification. In addition, they would have the skills and knowledge to ensure appropriate actions are taken to mitigate the impact on the IACS network.

- **IT Support (Tier 2, Tier 3)**
  IT technical experts such as the system administrators, network administrators, and cyber security specialists could be involved in incident response when cyber security incident impact extends out to the Corporate network. IT Support would have the skills and knowledge to ensure appropriate actions are taken to mitigate the impact on Corporate IT Systems. IT Support should notify the IACS cyber incident to isolate the OT network from the IT network as a possible initial response action.


https://t.me/learningnets

- **Legal Department (Tier 2)**
  Legal experts could review incident response plans, policies, and procedures to ensure compliance with the law. During an incident response, CSIRT may involve the legal department if there is reason to believe that an incident could have legal ramifications. The activities could include evidence collection, prosecution of a suspect, or a lawsuit.
- **Public Affairs and Media Relations (Tier 2)**
  The corporate communication department may be involved in a cyber incident response depending on the nature and the impact of the incident. The team would most adequately handle communication with the public and the media.
- **Finance (Tier 2)**
  Finance is responsible for managing costs and accounts. This includes managing payroll for CSIRT personnel and other required resources.
- **Human Resources (Tier 2)**
  Human Resources or HSE typically becomes involved as a safety officer in CSIRT to ensure the safety of all CSIRT members and the public.
- **Physical Security and Facilities Management (Tier 2, Tier 3)**
  Some cyber security incidents could occur through a physical compromise or a combination of logical and physical attacks. The CSIRT would then require an assistant from Physical Security or Facilities Management to secure or gain access to the compromised area.

### 2.1.2 Identifying and Classifying IACS Assets

IACS asset identification should provide enough details such that risk assessment and cyber asset classification can be performed.

An asset owner should be identified to be held responsible and accountable for each cyber asset. Although an asset owner may not have property rights to the cyber asset, they are still responsible for its production, development, maintenance, use, and security.

> The interdependency of assets for different cyber security criteria (e.g., availability or safety) should be identified. Similarly, the processes that depend on cyber assets should also be identified. Assigning value levels to assets is done by asset owners, cyber security specialists, and sometimes process owners.

Asset Security Zoning is the physical and logical grouping of the cyber assets with similar cyber security requirements. Different methods can be used to group the cyber assets. For instance, these groupings may be based on security criteria, asset valuation, the extent and coverage of their support to different organizational tiers, and business operations, etc.

For example, cyber assets can be classified into three security zones based on asset valuation: High, Medium, and Low.

**Table 1: Example of Asset Security Zones**

| Level | Description |
|---|---|
| High | The asset has an impact on safety, multiple business processes/units, or external systems/organizations. |
| Medium | The asset has an impact on a single business process/unit. |
| Low | The asset has minimal impact on business operations. |

As the threats to, and criticality of, cyber assets change over time, it is important to regularly update the documented risks assessed, associated security criteria and/or valuation of cyber assets, and subsequent changes to the Asset Security Zoning.

For more details on one approach for asset classification and risk assessments, refer to BBA's *IACS Cybersecurity Risk Methodology* [4].


https://t.me/learningnets

## 2.2 Incident Classification

This section describes how to assess and classify cyber security incidents, which will trigger the appropriate incident response plans and formulate the CSIRT.

A cyber security incident must be declared before proceeding with incident classification. Companies must rely on technical expertise from IACS / OT support team to investigate cyber security or system events and declare a cyber security incident when appropriate.

A cyber security incident classification method is required to assess the severity level of an incident consistently and objectively. The assessment approach described in the following sections is an example of the methodology used to achieve this.

### 2.2.1 Incident Types

The incident response assessment begins by identifying the types of cyber security incidents that could occur in the IACS environment. Incident types should be pre-defined by the organization to suit its own needs. The incident type can be categorized based on different factors, such as the techniques used, the vector of compromise, the type of assets that are compromised, etc.

For example, Table 2 shows incident types based on some of the attack tactics and techniques described in MITRE ATT&CK for Industrial Control Systems [5].

**Table 2: Example of Incident Types Based on MITRE ATT&CK Techniques**

| Tactic | Incident Type | | | |
|---|---|---|---|---|
| Initial Access | Data Historian Compromise | Drive-by Compromise | Engineering Workstation Compromise | Exploitation of Remote Services |
| Persistence | Modify Program | Brute Force I/O | Project File Infection | Valid Accounts |
| Privilege Escalation | Exploitation for Privilege Escalation | Hooking | | |
| Evasion | Change Operating Mode | Spoof Reporting Message | Rootkit | Masquerading |
| Discovery | Network Connection Enumeration | Network Sniffing | Remote System Discovery | Remote System Information Discovery |
| Lateral Movement | Exploit Default Credentials | Exploitation of Remote Services | Lateral Tool Transfer | Program Download |
| Inhibit Response Function | Activate Firmware Update Mode | Denial of Service | Alarm Suppression | Block Command Message |
| Impair Process Control | Change Module Firmware | Modify Parameter | Spoof Reporting Message | Unauthorized Command Message |


https://t.me/learningnets

### 2.2.2 Impact Analysis

Impact Analysis is an estimate of the potential or realized losses associated with an identified incident to individuals, the organization, third parties, public safety, or the environment.

The actual or projected impact that a cyber incident would have on the organization's business operations can be categorized into six groups:

- Financial;
- Reputational;
- Legal and regulatory;
- Environmental;
- Opportunity;
- Health and safety.

The impact of a cyber incident can be scaled into different levels (e.g., very low, low, medium, high, and severe). Table 3 is provided as an example of the magnitude of each impact category.

**Table 3: Example of impact level**

| Impact Type | Very Low | Low | Medium | High | Severe |
|---|---|---|---|---|---|
| **Financial** | <$10,000 cost | <$100,000 and >$10,000 cost | <$1,000,000 and >$100,000 cost | <$10,000,000 and >$1,000,000 cost | >$10,000,000 cost |
| **Reputational** | 1-5 clients would have minor complaints | Local news being remembered for less than a year | Being in local news and communities from 1 to 5 years | Being in national or international headlines | Internationally recognized as the main cause of a disaster |
| **Legal and regulatory** | Getting regulatory warning | Minor fine or mandated to do a further audit | Temporary suspension of a license | Losing some licenses | Permanent voiding of practice license |
| **Environmental** | Controlled and contained hazard | Contained hazard that can be fixed in a few days | Local hazard that will last for a few months | Wide environmental damage that will last for years | Permanent environmental damage |
| **Opportunity** | Delaying new contracts | Dissatisfaction of some existing clients | Losing some contracts with a value under $100,000. | Losing contracts with value between $100,000 and $1,000,000. | Losing all business line opportunities |
| **Health and safety** | Temporary and minor injuries | Repeated injuries | Numerous injuries or loss of organ | Casualties | Numerous casualties |

Refer to BBA's *IACS Cybersecurity Risk Methodology* [4] for more details on the approach to determine the impact levels.

### 2.2.3 Severity Analysis

The severity of an incident can be determined based on a combination of incident types, the classification of the compromised cyber assets (i.e., the highest applicable security zone), and the impact analysis results. The evaluated severity will be used to invoke a certain level of the incident response plan.

The incident severity matrix in Table 4 demonstrates how the security zones of impacted assets map to an incident severity level based on the assessed incident impact.


https://t.me/learningnets

**Table 4: Incident Severity Matrix**

| | | | | | | |
|---|---|---|---|---|---|---|
| Asset Security Zone | **High** | Medium | Major | Major | Critical | Critical |
| | **Medium** | Minor | Medium | Major | Critical | Critical |
| | **Low** | Minor | Minor | Medium | Major | Major |
| | | **Very Low** | **Low** | **Medium** | **High** | **Severe** |
| | | **Impact** | | | | |

To expedite the assessment process during an actual incident, it is recommended to develop a template with predefined incident classifications based on possible incident types, asset security zones, impact types, and impact levels. The table below presents an example of one such template.

**Table 5: Example Incident Classification Template**

| Incident Description | Incident Type (Techniques) | Asset Security Zone | Impact Type | Impact Level | Incident Severity Class |
|---|---|---|---|---|---|
| Failed attempt to compromise a user | Valid Account | Medium | Financial | Very Low | Minor |
| Single user workstation compromised | Engineering Workstation Compromise | Medium | Financial | Low | Medium |
| Sniffers installed on IACS networks | Network Sniffing | High | Financial | Low | Major |
| Multiple user compromise, single privileged access | Exploitation for Privilege Escalation | High | Financial, Reputation | Medium | Major |
| Denial of Service on control systems, unexpected shutdown | Denial of Service, Service Stop | High | Opportunity, Financial | Medium | Major |
| Man-in-the-middle on control systems, malfunction | Man-in-the-Middle, Loss of Control | High | Environmental, Health, and Safety | High | Critical |


https://t.me/learningnets

## 2.3 Incident Response Team

Many functions must be fulfilled to effectively respond to a cyber security incident. As potential or actual incidents grow in scope and complexity, so to do the tasks related to each of these functions. To improve efficiency, these functions may be distributed between the members of the Cyber Security Incident Response Team (CSIRT).

This section details the typical structure(s) of a CSIRT, the framework that defines how they are governed, the services they provide, how CSIRT members are selected, and how communication with other groups and stakeholders is facilitated.

### 2.3.1 Team Structure

There are different incident response team structures that can be followed by organizations:

- **Central Incident Response Team:**
  A single team is responsible for handling all IACS cyber security incident response activities throughout the organization. This model is effective for small organizations and organizations with low geographic differentiation in computing resources.
- **Distributed Incident Response Teams:**
  Multiple teams are employed, each responsible for handling cyber security incident response activities of a particular logical and / or physical segment of the organization. A single entity should be responsible for coordinating these teams to have consistent incident response processes across the organization, share knowledge and advice among teams, and manage the more complicated incidents with a more holistic perspective. CSIRT members often consist of people with primary roles outside of incident response. They may be called upon to provide support to the primary CSIRT members when needed.

Incident response teams can have different staffing models:

- **Employees:**
  Perform all cyber security incident response activities with limited external support.
- **Partial Outsourcing:**
  Specific incident response tasks can be outsourced. Examples of common arrangements may include:
  - Using an offsite Managed Security Services Provider (MSSP) to monitor technical systems. The MSSP monitors suspicious activities and reports incidents to the organization's CSIRT.
  - Performing basic incident response tasks in-house. If suspicious activities or incidents are detected, contractors are utilized to assist with the handling of incidents.
- **Complete Outsourcing:**
  Completely outsource the cyber incident response program, typically to an on-site contractor. This model is usually employed when the organization needs a full-time incident response team but does not have the required available qualified staff. Organization employees would typically supervise the outsourced program / tasks.

The decision to use a particular team structure and staffing model depends on the size, complexity, and incident response needs of the organization. For instance, a larger organization with multiple business units will benefit from a coordinated, decentralized approach.


https://t.me/learningnets

### 2.3.2 Incident Command System (ICS) Framework

The Incident Command System is described as a framework for coordinating the CSIRT. Its purpose is to allow the cyber security incident response program to be integrated with industry-recognized incident response methodologies.

Tasks that are managed using the ICS framework may include:

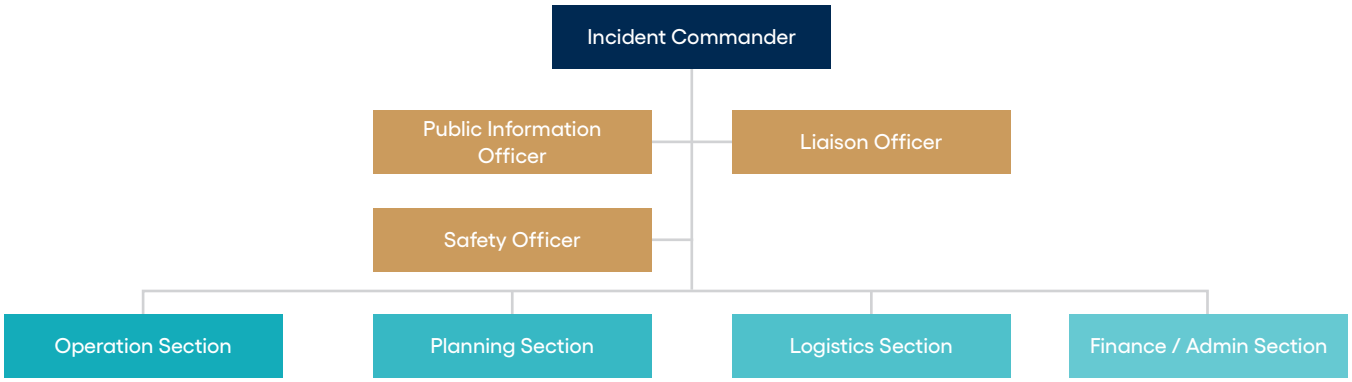
- General organization and governance of the incident response;
- Planning activities, including the evolution of the plans as the situation changes;
- Setting periodic response goals or objectives;
- Providing logistical support;
- Maintaining safety during operations;
- Tracking and documentation of the cyber security incident;
- Management of available personnel and resources;
- Performing financial duties such as tracking costs and payroll;
- Communicating with relevant internal and external parties.

#### 2.3.2.1 Incident Command System Team Structure

The Command Section is responsible for setting the short and long-term goals of the CSIRT, facilitating communication, and high-level management of the various groups and teams involved in incident response.

As shown in Figure 3, there are four primary command staff roles in the ICS structure:

**Figure 3: Incident Command System Structure**




- **Incident Commander (IC)**

  A highly qualified individual trained to lead the incident response. The IC is responsible for managing the overall incident, maintaining safety during the incident, providing information services to internal and external stakeholders, and coordinating with other participating agencies. The IC is the only role that must be filled for any given incident.

  For incidents that are sufficiently limited in scope, the IC may be capable of fulfilling all management functions. As incidents increase in complexity, some of these functions may be broken out into separate sections.


https://t.me/learningnets

- **Public Information Officer (PIO):**
  Serves as the channel for communication to internal and external stakeholders such as the senior management and the media. Reports directly to the IC. Figure 4 presents several potential contacts that would fall within their responsibilities.

**Figure 4: Public Information Officer Communication Channels**


- **Safety Officer:**
  Monitors and manages safety issues related to the cyber security incident to ensure the safety of all CSIRT members and the public. Reports directly to the IC.
- **Liaison Officer:**
  The primary contact for initiating and maintaining contact with government agencies, regulatory authorities, and mutual aid partners during an incident.

As shown in Figure 3, below the Command Section are four Functional Sections that are responsible for the functional aspects of the incident command response:

- **Operations Section:**
  Directly manages the resources who conduct the various incident response activities.
- **Planning Section:**
  Develops the plans which will be used to achieve the goals prescribed by Incident Command. Aggregates information relevant to the development of these plans. Evaluates the resources available to complete tasks.
- **Logistics Section:**
  Provides resources, services, and other miscellaneous support required during the incident response process.
- **Finance / Administration Section:**
  Manages costs and accounting needs associated with incident response.

Each Functional Section is managed by a section chief who oversees its activities. The section chief also ensures ongoing communication with the Incident Commander and command staff.

#### 2.3.2.2 Incident Management Governance

Following the Incident Command System (ICS), the CSIRT will be governed by eight key governing principles:

- **Unity of Command:**
  All members in the CSIRT will report to only one direct supervisor (e.g., Incident Commander, Operations Chief, Planning Chief, etc.). This reduces the potential for conflicting orders, increases operational efficiency, improves accountability, and promotes information sharing. The Incident Commander leads the incident response and has overall responsibility for its management.
- **Transfer of Command:**
  If the incident response takes place over a long period, it may be necessary to perform a transfer of command. The process must include a briefing that captures all key information to safely and effectively continue incident response operations.
- **Use of Common Terminology:**
  CSIRT members should be familiar with the common terminology used in incident management. This is especially important for team cohesion and communications in a multidisciplinary CSIRT.
- **Management by Objective:**
  Incidents should be managed by working towards specific goals. Under the direction of the Incident Commander, the CSIRT establishes overarching objectives. These objectives are then used as the basis for developing strategies, plans, and assignments.
- **Flexible and Modular Organization:**


https://t.me/learningnets

The CSIRT structure follows the ICS – it can expand or contract as required to suit the incident scope, available resources, and threat levels.

- **Manageable Span of Control:**
  Ideally, any single person's span of control in the CSIRT structure should only include three to seven individuals. This improves the efficiency of the command structure and avoids overloading an individual with supervisory duties.
- **Incident Action Planning:**
  A centralized and coordinated Incident Action Plan (IAP) should account for all response tasks. It should communicate overall incident objectives, strategies, and priorities. The IAP does not need to be a written plan – the IC decides to incorporate a formal written IAP based on incident duration and complexity.
- **Incident Facilities and Locations:**
  The Incident Commander will identify and select suitable incident handling locations based on the type and complexity of the cyber security incident. These locations would be for facilities such as the Emergency Operations Centre (EOC), bases, camps, staging areas, etc. To expedite the location selection process during an actual incident response, organizations should identify potential locations in advance. Ideally, the EOC should be in a location that is easily accessible to CSIRT members and near the main IACS / OT cyber security and network team.

### 2.3.3 Services

Services offered by the CSIRT may include, but are not limited to:

- **Incident Detection:**
  Incident detection is a common responsibility of the CSIRT, as it may help identify potential or actual attack vectors and otherwise aid information gathering. Knowledge of attack vectors may also assist containment efforts.
- **Incident Response:**
  This can be considered the primary function of the CSIRT. The CSIRT creates incident response plans in preparation for potential cyber security incidents. When an incident occurs, these plans are then executed accordingly. To prevent the situation from escalating, it is important to ensure that the scope of the incident is limited as much as possible via containment activities. Where possible, the source of the incident is then addressed via removal where possible. Finally, the system is restored to its original state such that normal operation can resume. Refer to Section 3.3.5 for more details.
- **Information Sharing:**
  The CSIRT often shares information with external user groups, as well as internally. This effort ensures that relevant parties are kept aware of the situation and any associated threats. As part of this, the CSIRT may also be responsible for gathering information regarding the incident.
- **Post-Incident Reporting:**
  After the incident has concluded, the CSIRT is typically responsible for documenting the details of the incident response process, including areas of strength and weakness. These findings may be used to author a lessons learned report, which would improve future incident response.

### 2.3.4 Develop CSIRT Formulation Guide

Prior to an incident, groundwork must be completed to establish the foundation for the CSIRT. This includes defining the scope of the CSIRT's mission, its authority within the organization, key contacts for the group, organization / structure, and the skills / services they offer.

As previously stated, the structure of the CSIRT is based on the ICS framework (see Figure 3). When an incident is identified and classified, the first Incident Commander (IC) would be assigned and the response process is initiated. The person who declares the incident usually takes the first IC role and can transfer of authority if / when needed. Depending on the severity of the incident (see Section 2.2.3), the Incident Commander will assign appropriate personnel to lead each of the core sections. In general, as an incident increases in severity, higher tiers of management in the organizational structure will become involved.

An example of how these roles may be assigned is shown in Table 6.


https://t.me/learningnets

**Table 6: Example CSIRT Formulation Table**

| | | Incident Severity | | | |
|---|---|---|---|---|---|
| | | Minor | Medium | Major | Critical |
| ICS Role | **Incident Commander** | Tier 2 OT Systems | Tier 2 Operations | Tier 2 Operations | Tier 2 Operations |
| | **Public Information Officer** | N/A | Tier 3 Human Resources System | Tier 2 Human Resources | Tier 2 Human Resources |
| | **Safety Officer** | N/A | Tier 3 Safety Controls | Tier 2 Health, Safety, and Environment | Tier 2 Health, Safety, and Environment |
| | **Liaison Officer** | N/A | Tier 3 Human Resources System | Tier 2 Human Resources | Tier 2 Human Resources |
| | **Operations Section Chief** | N/A | Tier 3 OT Systems | Tier 3 OT Systems | Tier 3 OT Systems |
| | **Planning Section Chief** | N/A | Tier 3 Operations | Tier 3 Operations | Tier 3 Operations |
| | **Logistics Section Chief** | N/A | Tier 3 Operations | Tier 3 Operations | Tier 3 Operations |
| | **Finance Section Chief** | N/A | Tier 3 Payroll System | Tier 2 Financial | Tier 2 Financial |

### 2.3.5 Communications

Maintaining good communication between groups is extremely important during incident response. A communications plan is key to this, since it describes when certain stakeholders would be brought into the response effort; it presents clear criteria for escalating the incident response.

The requirements for facilitating good communication will vary, as each organization has its own needs. Measures to improve communication may include:

- Reserving specific meeting rooms for CSIRT use only, once an incident has been declared.
- Having an alternate work location in the event that the primary work location becomes unusable or unsafe for any reason.
- Creating templates to standardize regular reports or information sharing between teams.
- Creating guidelines on what is considered an appropriate level of detail for the intended audience. This will vary greatly between groups such as technical subject matter experts and the general public.
- Creating processes to review and approve material before it is disseminated to stakeholders.

A cyber security incident may also affect an organization's capability to communicate. For instance, if a network is isolated to prevent the spread of malware, email or other collaborative tools may become unusable from within that network. Similarly, compromised administrative or service accounts may cripple communication tools if they rely on those accounts for certain functions.

Consequently, it is recommended that alternate communication channels be made available for redundancy. These channels would be used only if the primary modes of communication become unavailable. To prevent confusion, the incident response plan should clearly define when and in what situations each alternate mode of communication should be employed.


https://t.me/learningnets

Examples of alternate communication channels could include:

- News posts on a corporate intranet site;
- Internet connections through less conventional media, such as cellular and satellite;
- Conventional telephone via landlines;
- Cell phones;
- Handheld radios.

The incident response must also be considered at the site level. If communications between the site and primary incident command are severed, the site must be capable of functioning independently. As a result, it is prudent to create incident response procedures specific to that site. In addition, a local Incident Commander should also be appointed, as they would need to take command if communications are lost. The conditions required for this autonomous remote response must be clearly defined, and the decisions to accept these conditions should be well documented.

## 2.4 Incident Response Planning

An organization should have a formal and coordinated approach for responding to incidents, including incident response policies and plans that provide the roadmap for implementing the incident response tasks. Each organization needs a cyber security incident response policy that suits the organization's mission, size, structure, and functions. It also needs incident response plans that meet the unique requirements of its incident response policy.

Incident Response Plans (IRP), guidelines for formulation of the CSIRT, and communication structures should be designed to be scalable. They should also be capable of integrating with other organizational incident response processes beyond the scope of IACS / OT teams. By utilizing the ICS framework, integration with incident response processes external to the organization (e.g. national incident response programs) can also be achieved.

### 2.4.1 Policy

A cyber security incident response policy should provide the formally documented principles and intentions used to direct decision-making and ensure consistent and appropriate implementation of this policy's standards, guidelines, processes, and procedures.

Any cyber security incident response policy should be part of the organization's cyber security strategy and should support the organization's existing mission and be in line with already existing policies and procedures.

The organization should implement the cyber security incident response policy that outlines the processes, responsibilities, authority, awareness and training initiatives, and reporting lines when a cyber security incident occurs. The policy should be reviewed regularly to be aligned with the latest organizational structure, standard, processes, and technology.

An organization should direct its cyber security incident response policy at every person having legitimate access to cyber systems and related locations.

Before the cyber security incident response policy is formulated, the organization should identify the following regarding its cyber security incident management:

- Objectives;
- Interested parties, both internal and external;
- Specific incident types and vulnerabilities that need to be highlighted;
- Any specific roles that need to be highlighted;
- Benefits to the whole organization and its departments.

A successful cyber security incident response policy should be created and implemented as an enterprise-wide process. To that end, all stakeholders or their representatives should be involved in the development of the policy from the initial planning stages through the implementation of any process. This may include upper-level management, legal advisors, public relations and marketing staff, departmental managers, security staff, site managers and specialists, ICT staff, and helpdesk staff.


https://t.me/learningnets

> The cyber security incident response policy should be sponsored by a member of senior management, with commitment from all top management. Ensuring continued management commitment is vital for the acceptance of a structured approach to cyber security incident management. Personnel needs to recognize an incident, know what to do, and understand the benefits of the approach by the organization. Management needs to support the cyber security incident policy to ensure that the organization commits to resourcing and maintaining the incident response capability.

The cyber security incident response policy should be made available to every employee and contractor and also should be addressed in cyber security awareness training.

The cyber security incident response policy should address, but is not limited to, the following topics in high-level:

- The purpose, objectives, and the scope (to whom it applies and under what circumstances) of the policy.
- The Incident Response Process Owner and review cycle.
- The importance of cyber security incident management to the organization and top management's commitment to it.
- Definition of cyber security incident and description of the types of cyber security incidents.
- Description of how incidents should be reported, including what to report, the mechanisms used for reporting, where and to whom to report.
- Overview of the incident response process flows from detection through reporting, information collection, analysis, response, notification, escalation, resolution, and lessons learned.
- A requirement for post cyber security incident resolution activities, including learning from and improving the process, following the resolution of cyber security incidents.
- Defined roles, responsibilities, and decision-making authority for each phase of the cyber security incident response process and related activities.
- Overview or reference to the document describing the event and incident classification, severity ratings, and related terms.
- Continuous monitoring tasks and requirements for IACS environment, incident response processes with performance measures, and preservation of electronic evidence in case it is required for legal prosecution or internal disciplinary action.
- Authority granting the CSIRT access to the outputs of the monitoring task or the ability to request logs as needed from other parts of the operation.
- Overview of the CSIRT in line with ICS framework, describing the CSIRT organizational structure, key roles, responsibilities, authority, a summary of duties including, but not limited to, the following:
    - Reporting and notification requirements related to incidents that have been confirmed;
    - Briefing senior / executive management on incidents;
    - Dealing with inquiries, instigating follow up, and resolving incidents;
    - Liaising with the external stakeholders;
    - Requirement and rationale for ensuring all cyber security incident response activities performed by the CSIRT are properly recorded.
- Communications and information sharing requirements which outline how and when information related to incident response activities can be shared and with whom. Information sharing should follow legal requirements, organizational confidentiality requirements, minimal disclosure, and only the relevant legislation. The scope, circumstances, and purpose of the information sharing need to be described.
- Information storage and handling requirements that mandates records, data, and other information related to investigations be stored and handled securely. This can be integrated into the organizational document classification schema if the organization has that in place.
- Requirement about collaborations across the organization to detect, analyse, and respond to cyber security incidents.


https://t.me/learningnets

- Description of oversight or governance structure, in line with ICS framework, and the authority and duties of the commander.
- Links to organizations that provide specific external support such as forensics teams, legal counsel, IT operations, etc.
- Referring to the legal and regulatory compliance requirements or mandates associated with cyber security incident response activities.
- Requirements of the cyber security incident response awareness and training program. This should include any incident response training mandates and requirements for CSIRT members and staff-related employee awareness training.

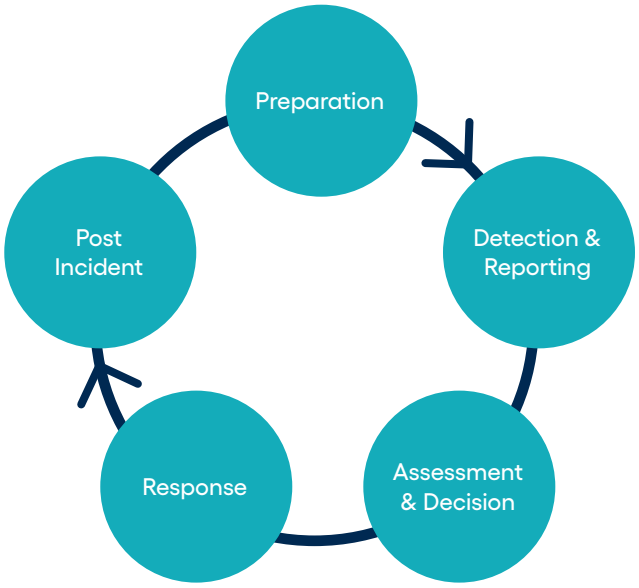
### 2.4.2 Plan and Procedure

An organization should use the IACS Cyber Security Incident Response Plan (IRP) as a guide for the following:

- Responding to IACS cyber security events;
- Determining whether the cyber security event becomes a cyber security incident;
- Managing IACS cyber security incidents to the conclusion;
- Reporting to management as required;
- Documenting and storing information during the incident response process as required;
- Sharing information with internal and external groups or organizations, based on rules and circumstances;
- Identifying lessons learned and any improvements to the plan and/or security in general that are required;
- Implementing the identified improvements.

The IRP comes into effect whenever a cyber security incident is detected. A typical cyber security IRP lifecycle is shown in Figure 5.

**Figure 5: Cyber Security Incident Response Life Cycle**




#### 2.4.2.1 Preparation

- A standardized approach to cyber security event / incident classification to enable the provision of consistent results. In any event, the decision should be based on the actual or adverse impacts on the organization's business operations.
- A communication structure and database for the exchange of information, share reports / alerts, compare results, improve alert information, and enable an accurate view of the threats and vulnerabilities. The format of communication structure can vary from using simple document sharing to sophisticated application tools, depending on the size of the organization.
- A communication structure and guidance for external information sharing as agreed with the organization's public affairs office, legal department, and senior / executive management.
- Escalation guidance, including the required conditions of escalation during each relevant process, the target role that the escalation is happening to, and the related procedures. Based on this guidance, anyone assessing a cyber security event, incident, or vulnerability should know under which conditions it is necessary to escalate matters and to whom it should be escalated.


https://t.me/learningnets

- Procedures to log all cyber security incident response activities and conduct the log analysis by designated personnel.
- Procedures to ensure that the cyber security event, incident and vulnerability tracking and cyber security report updates are maintained in change management system.
- Procedures for cyber security evidence analysis.
- Technical and procedural mechanisms to prevent cyber security incident occurrences, reduce their likelihood, and deal with cyber security incidents as they occur. These mechanisms can be established or implemented. They include the guidance for using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
- Procedures associated with the technical and organizational mechanisms that are established, implemented, and operated to prevent cyber security incident occurrences, reduce their likelihood, and deal with cyber security incidents as they occur.
- Awareness and training program material for the cyber security event, incident and vulnerability management.
- Testing procedures for the cyber security incident response plan.
- The plan of assigning roles from organizational structure to cyber security incident response team (CSIRT) based on Incident Command System (ICS).
- The responsibility terms of the CSIRT and its members.
- Important contact information.

#### 2.4.2.2 Detection and Reporting

- Requirements for detection and reporting of cyber security incidents in order to support the development of processes to find or accept information about the cyber security incidents.
- The minimum criteria for acceptance of a cyber security event and incident detection report should be defined before the planning process. It should include identifying affected assets, the statement of suspected or confirmed event / incident, and the time received. The planning process should include the method for returning reports that have insufficient information. Reporting output should be defined in the context of the organization, the cyber security incident response policy, and the assignment of technical and management roles.
- Detecting and reporting the occurrence of cyber security events (automatic or manual).
- Responding to incorrect use of the reporting process.
- Collecting the information about cyber security events.
- Detecting and reporting cyber security vulnerabilities.
- Recording collected information in the cyber security database.

#### 2.4.2.3 Assessment and Decision

- Requirements for assessment and decision making in order to support the development of processes to evaluate and direct actions in response to cyber security incidents.
- Defining the minimum information for identification and classification of a cyber security incident by the process owner prior to the development of assessment and decision processes. This allows response planners to develop consistent processes for completeness and classification of the reported events. Define the requirements to differentiate between true positive and false-positive reports.
- Conducting the initial assessments of cyber security events by the point of contact, in order to decide whether events should be classified as cyber security incidents and escalate if needed, using the cyber security event / incident classification.
- Assessing cyber security events by the CSIRT in order to confirm whether an event is a cyber security incident or not. The details of the suspected incident type and affected assets are confirmed using the cyber security event/incident classification scale. It needs to be decided how the confirmed cyber security incident should be handled, by whom, in what priority, and escalation level.


https://t.me/learningnets

- Assessing cyber security vulnerabilities (that have not yet been exploited to cause cyber security events and potential cyber security incidents), with decisions made on which need to be dealt with, by whom, how, and in what priority.
- Recording all assessment results and decisions in the cyber security database.

#### 2.4.2.4 Responses

- Requirements for responding to cyber security incidents.
- Define the priority of cyber and cyber security systems, the impact of each intrusion type, damage scale, intrusion alarm level, and severity levels before response planning. These definitions should be consistent with assessment and decision preparations and enable the CSIRT manager to assign tasks to responders.
- Define classes of response prior to the planning process, organized by cost, time, technical resource minimums, to be able to assign response classes to assessed incidents. Response processes may need actions that are an immediate or deferred, single or cyclic sequence of incident tasks.
- Determine if the cyber security incident is under control by the CSIRT,
    - If the incident is under control, initiate the required response, either immediately or at a later time, or
    - If the incident is not under control or it is going to have a severe impact on the core services, escalate the situation to the crisis activities.
- Develop a map of all internal and external functions and entities that should be involved in the incident management process.
- Contain and eradicate the cyber security incident to mitigate or prevent the scope and impact of the incident from growing.
- All involved activities should be properly logged for later analysis. Conduct cyber security evidence analysis, as required.
- Escalate, as required.
- Procedures to ensure that the cyber security response activities are maintained in the change management system.
- Communicate the existence of the cyber security incident and any relevant actions to other internal and external entities based on the designed communication structure.
- Accept mitigating the cyber security vulnerabilities.
- Formally closing the incident and recording it in the cyber security database once it has been successfully handled.

#### 2.4.2.5 Post Incident

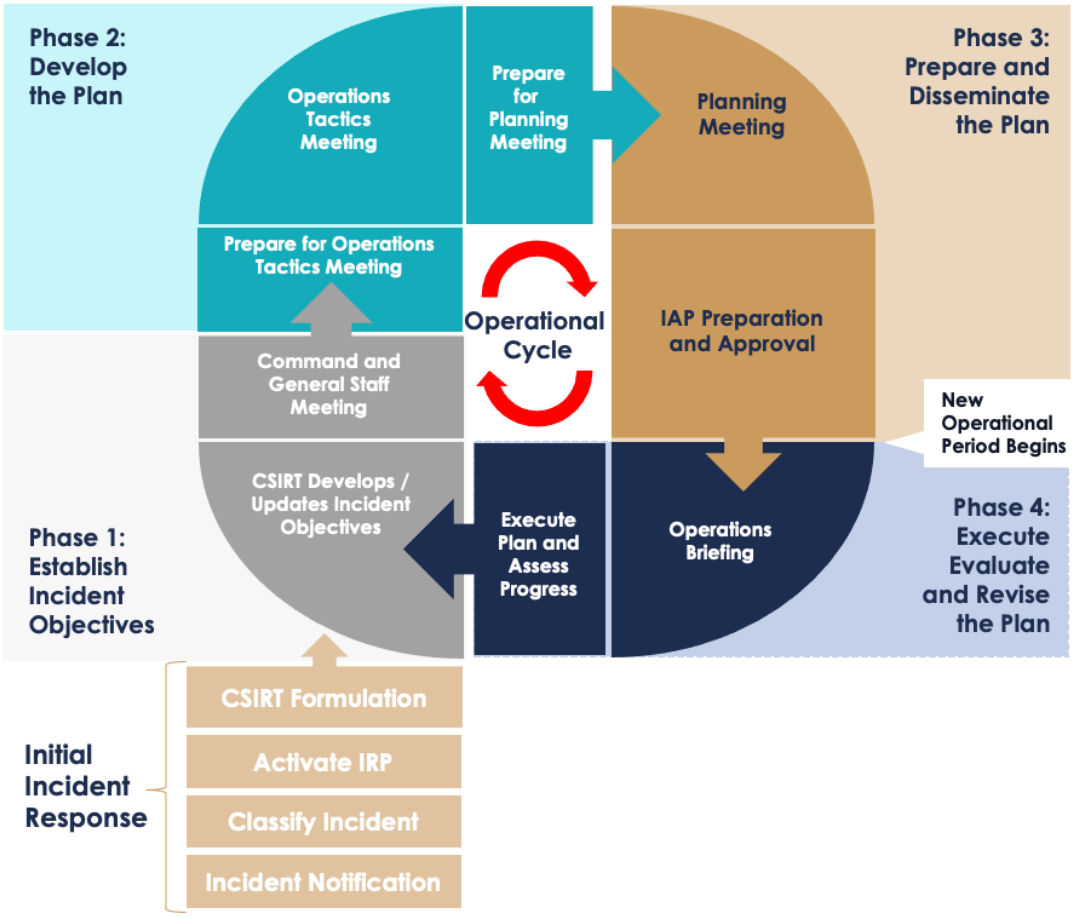
- Identify the lessons learned from cyber security incidents and vulnerabilities.
- Identify, review, and improve the cyber security policies, procedures, and controls, as a result of the lessons learned.
- Identify, review, and improve the cyber security risk assessment and management as a result of the lessons learned.
- Review the effectiveness of processes, procedures, reporting formats, the organizational structure, and planning related to assessing and recovering from each cyber security incident and handling cyber security vulnerabilities.
- Update the cyber security database.
- Share the results of the review within a trusted community if the organization wishes to.


https://t.me/learningnets

### 2.4.3 The Operational Cycle

As defined by the ICS, the Operational Cycle is a cyclical process that consists of establishing objectives, execution tactics, plans, and briefings to ensure that an adequate Incident Action Plan (IAP) is developed and executed. Each cycle is referred to as an Operational Period. The Operational Cycle ensures effective communications between the CSIRT members and promotes informed, collaborative decisions during the incident response, going through the response stages (Section 3.3.5).

**Figure 6: Incident Response Operational Cycle**




**The Incident Action Plan (IAP):**

The IAP is a written plan containing objectives, action items, and execution directions for managing incident response. The IAP is continuously reviewed, evaluated, and revised throughout the Operational Cycle. While the IRP provides an overall Incident Management strategy and guidance, the IAP focuses on real-time incident response actions required during the actual incident response, including detailed incident analysis, containment, eradication, and recovery. The IAP is considered a work-in-process document during the Operational Cycle phase.

**Planning Process:**

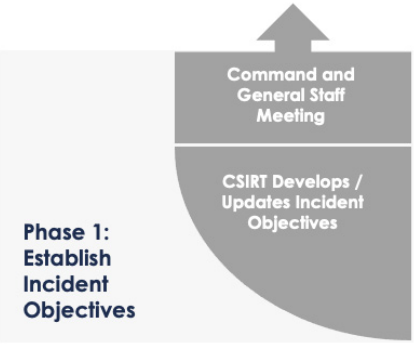
The Operational Cycle is an ongoing planning process that provides guidance for strategic, operational, and tactical planning that includes all steps that CSIRT should take to develop, disseminate, and execute an IAP.

The Operational Cycle has four separate phases:

- Establish Incident Objectives;
- Develop the Plan;
- Prepare and Disseminate the Plan;
- Execute, Evaluate, and Revise the Plan.


https://t.me/learningnets

### Phase 1: Establish Incident Objectives




The first phase of the Operational Cycle begins with formulating and prioritizing incident objectives and identifying strategies to mitigate or alleviate the incident. Establishing SMART objectives is recommended to provide a well-structured approach to developing a work plan and to succinctly communicate the intended goals to the CSIRT and other stakeholders.

**Table 7: SMART Objectives**

| | | |
|---|---|---|
| **S** | Specific | Clearly outline in a statement precisely what is required. What are we going to do, with whom, and for whom? |
| **M** | Measurable | Include how the CSIRT will monitor and measure how well the objectives are being achieved. |
| **A** | Action-Oriented | Use action verbs to describe the expected outcome or achievement. |
| **R** | Realistic | Ensure the outcome is achievable given the current incident situations or available resources. |
| **T** | Time frame | Include when the objective is expected to be achieved. |

The Command and General Staff meetings are held in the following manner:

- The Planning Section Chief brings the meeting to order and reviews the agenda.
- Each Section Chief conducts situation status briefing including their objectives.
- If necessary, the Safety Officer provides a safety briefing.
- The Incident Commander:
  - Leads the incident objective discussion with the Section Chiefs.
  - Reviews incident priorities, restrictions, and limitations.
  - Finalizes the list of objectives for the Operational Period.
  - Reviews any open action items and assigns resources.
  - Decides and communicates when the next Operations Tactics Meeting will be held.

### Phase 2: Develop the Plan


The second phase consists of developing the tactical plans and strategies to achieve selected objectives for the Operational Period. The resource utilization, contingency plans, and logistics support required to accomplish the objectives are analyzed, discussed, and determined. This phase consists of preparing and conducting the Operations Tactics Meeting and preparing for the Planning Meeting in the next phase.


https://t.me/learningnets

The **Operations Tactics Meetings** are held in the following manner:

- The Planning Section Chief brings the meeting to order and reviews the agenda.
  - The Incident Commander oversees the meeting; however, the Section Chiefs mainly lead the meeting discussion.
  - Each Section Chief conducts a short situation briefing.
  - The Planning Section Chief reviews the current incident objectives.
  - The Operational Section Chief reviews and addresses the resource utilization, contingency plans, and logistics support required to accomplish the objectives.
  - The Safety Officer discusses and resolves any safety issues.
  - The Logistics Section Chief discusses and resolves any logistics issues.
  - The Finance Officer Chief discusses and resolves any finance issues.
  - The Operational Section Chief reviews any open or incomplete action it ems.
  - The Planning Section Chief decides and communicates when the next Planning Meeting will be held.

### Phase 3: Prepare and Disseminate the Plan


The third phase consists of developing a detailed plan of actions required to meet the incident objectives. The IAP contains the incident objectives, strategies, assignments, action items, and execution directions determined by the previous two planning phases. The IAP should be prepared in a format that is appropriate for the incident complexities. For example, for small and low classified events, a simple outline document or even a verbal plan would be sufficient; however, larger and high classified events may require a formal written IAP document be prepared. The Planning Section is responsible for developing the IAP.

The **Planning Meetings** are held in the following manner:

- The Planning Section Chief brings the meeting to order and reviews the agenda.
- Each Section Chief conducts a short situation briefing.
- The Planning Section Chief reviews the incident objectives, strategies, and relevant planning decisions made.
- The Operations Section Chief reviews the current operation and the proposed work plan.
- The Incident Commander and the Section Chiefs review the proposed plan to ensure that the incident objectives and priorities are met.
- The Planning Section Chief requests the Command and General Staff members' commitment to the proposed plans in the IAP.
- The Planning Section Chief request the approval of IAP from the Incident Commander.
- The Planning Section Chief decides and communicates when the next Operations Briefing will be held.

### Phase 4: Execute Evaluate and Revised the Plan



https://t.me/learningnets

The fourth phase includes the Operations Briefing followed by execution of planned activities as defined by the approved IAP. The purpose of the Operations Briefing is to have the last opportunities to review the approved IAP with the CSIRT before teams are dispersed to execute the plans. The General Staff should regularly monitor the work progress to ensure alignment with the planned progress and objectives.

The **Operations Briefings** are held in the following manner:

- The Planning Section Chief brings the meeting to order and reviews the agenda.
- The Planning Section Chief reviews the incident objectives of the approved IAP.
- Incident Commander can provide any incident situation updates.
- The Planning Section Chief solicits final comments and adjourns the briefing.

## 2.5 Monitoring the IACS Environment

This incident response component defines the scope of monitoring as it pertains to the IACS environment. The organization controls some changes to the inputs of this activity (e.g. assets). Other changes can happen without notice, such as threats, vulnerabilities, or consequences. As such, constant monitoring is necessary to detect adverse changes as early as possible.

Assets, controls, vulnerabilities, and threats should all be monitored and evaluated to identify any changes in the context of the organization and to maintain an overview of the company's cyber security posture. Based on the level and type of changes detected, this can trigger an incident response plan, communications to stakeholders, and / or logging of the identified changes.

Monitoring must be an integral part of the incident response process to ensure that the various incident response activities are effective. It is necessary to ensure that the following are constantly monitored in IACS systems and environments:

- Assets that have been included in the incident response scope, using defined measures;
- Necessary modification of assets and asset values (e.g., due to changes in environment and requirements);
- New potential threats – both inside and outside the organization – that have not yet been assessed;
- Defined measures to evaluate the effectiveness of controls in place (e.g., frequency of incidents);
- Changes to potential impacts or consequences;
- The results of system evaluations, such as penetration testing, cyber security control assessment, identity and access assessment, etc.

Changes in the IACS environment can affect the impact and incident classification of previously reviewed incidents. Therefore, major changes should be a reason for a more specific review of incident classification. IACS environment monitoring activities should be performed regularly or constantly.

### 2.5.1 Documentation of Monitoring Activities

Cyber security incident response processes and their outputs should be documented through an appropriate mechanism. In this process, the scope, criteria, factors, and metrics of documentation are taken from documentation requirements. This mechanism should select some factors from the data generated by each process, which allows comprehension, investigation, analysis, and repetition of considerable events within that process or inter-process communications.

All events, changes, results, regulations, thresholds, requirements, decisions, responses, effects, processes, and communications get recorded accordingly.

The information of all incident response processes, inter-process interactions, and information about the operational environment from internal and external sources are used to securely record a selected portion of that information and keep it reliably available.

This information is used in the incident response evaluation process, the review and improvement process, event monitoring processes, and the communication process.


https://t.me/learningnets

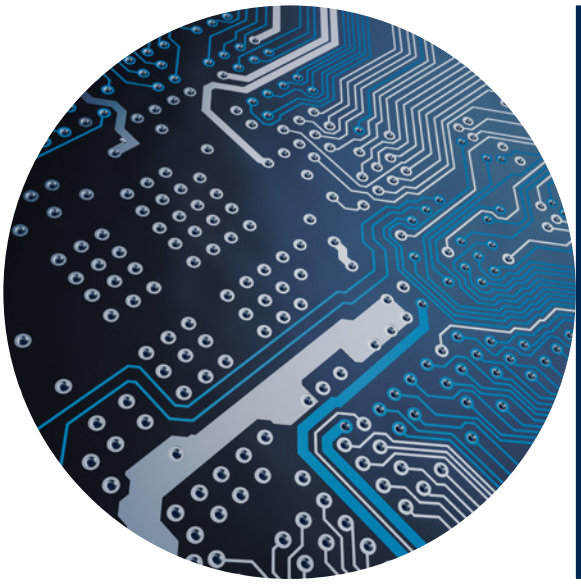
## 2.6 Evaluating the Incident Response Process

All IR processes should be continually examined and their effectiveness evaluated, along with their interdependency with the operational environment and other processes. The IR evaluation process can initiate the review and improvement process by identifying effectiveness measures and potential gaps, communicating to proper stakeholders based on the level and type of gaps detected in the process, and / or logging the identified process analysis and gaps.

The IR evaluation process analyzes individual and overall processes. The scope for the evaluation should be defined. Effectiveness metrics for each process should be designed with respect to the scope and requirements of that process. Responsibilities, requirements, and guidelines for assessment / monitoring roles also need to be defined (e.g., system evaluators, penetration testers).

The IR evaluation processes should include (but are not limited to):

- Regularly verifying that the criteria used to measure the incident prevention, detection and response are still valid and consistent with business and cyber security objectives, strategies, and policies.
- Verifying compliance with federal legislation, directives, regulations, policies, standards and guidelines.
- Regularly verifying that changes to the business context are taken into consideration adequately during the cyber security incident response process.
- Checking whether the planned and in-place incident responses are addressing the identified risks and vulnerabilities.
- Observing the incident response communication flow and measuring the effectiveness of the decision escalation flow.
- Checking incident response objectives to ensure it is in line with the business strategy.
- Observing the effect of changes in different incident responses on the behavior of cyber incidents.
- Observing resource availability for incident response with respect to identified incident plans.
- Evaluating the effectiveness of the asset monitoring process.
- Evaluating asset classification and the valuation process.
- Evaluating documented patterns, logs, and reports to extract near misses, substandard conditions, substandard practices, and deviance from standard procedures.
- Evaluating documented and non-documented details of processes, incidents, and log files to identify culture and competency gaps in various processes.
- Testing the Incident Response plans, analyzing the results, and mitigating the gaps in IRPs.




https://t.me/learningnets

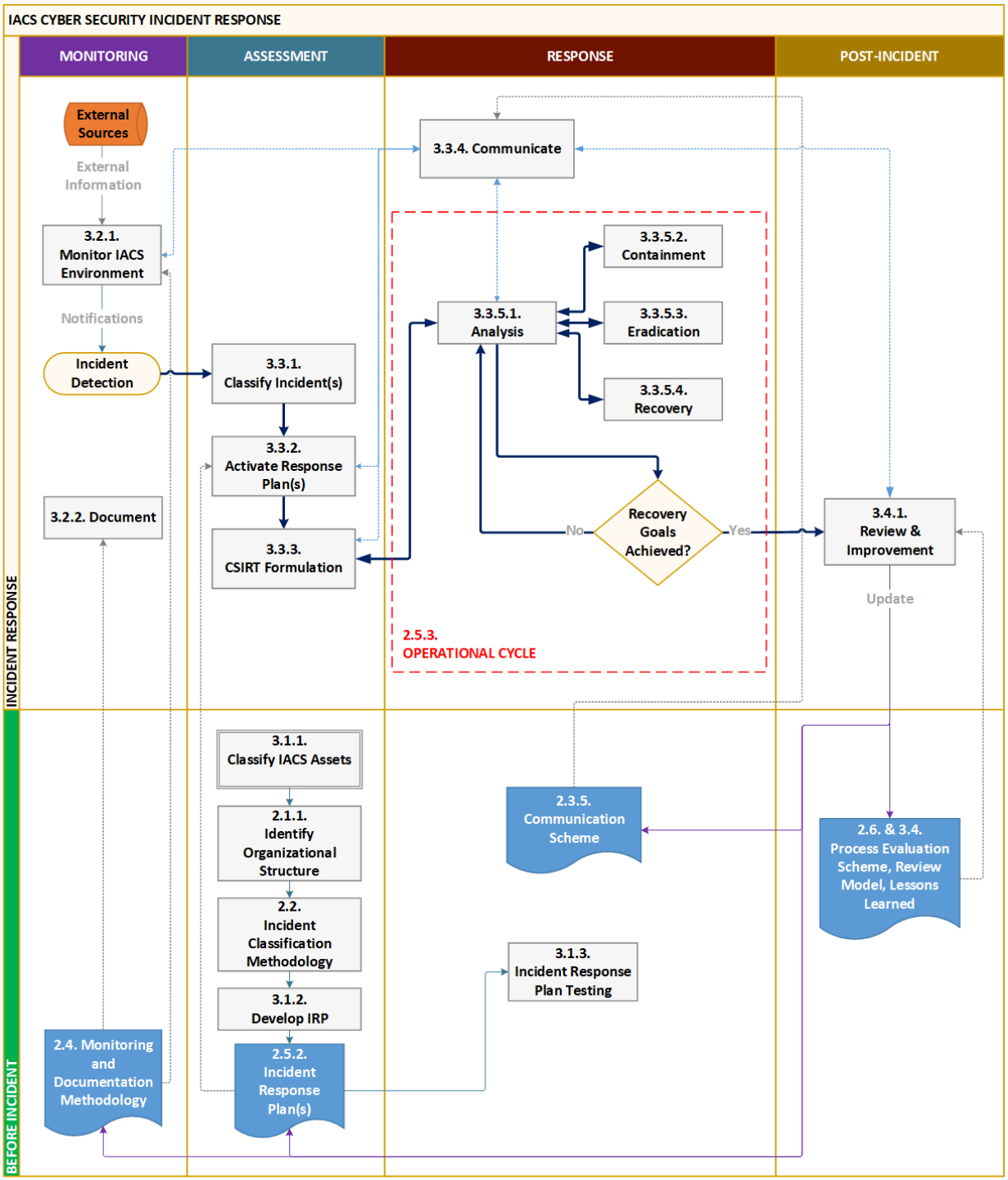
CHAPTER 3

# Processes

This chapter describes the process of managing cyber security incidents, including the preparatory work that must be completed before any incident has occurred, how monitoring should be conducted to detect an incident, the actions taken after detection as dictated by the IRP, and process improvements made after the incident has concluded.


https://t.me/learningnets

## Figure 7: Operational Cyber Security Incident Management Process





https://t.me/learningnets

## 3.1 Pre-Incident

### 3.1.1 Develop Incident Classification Guideline

- **Input:** Risk Assessment, IACS Asset Classification (Section 2.1.2), Incident Types (Section 2.2.1), Impact Analysis (Section 2.2.2)
- **Action:** Classify potential IACS cyber security incidents by identifying appropriate incident types for the IACS environment, analyzing their impact and severity on the organization.
- **Output:** Incident Classification Guideline, Incident Classification Template.

**Implementation guidance:**

The organization will first analyze and create a list of possible cyber security incident types that the organization's IACS environment could face. Of course, it is not possible to cover all types of incidents; however, having a comprehensive list covering a broad spectrum of incident types will later benefit the response to the actual incident by expediting the incident classification process. Following this step, impact analysis is conducted on each identified incident type to associate business operations impact value to the incidents. Finally, the incidents are classified into different severity levels. The severity is determined by the security zones of impacted IACS assets and the impact associated with the incident type.

A table of incident types, impact levels, asset security zones, and the pre-determined severity levels would form an *Incident Classification Template*. This template will set a basis for the incident classification that occurs after detecting a cyber security incident. *The Incident Classification Guideline* is a written document that outlines the incident classification methodology and the instruction on how to use the Incident Classification Template.

Refer to Section 2.2 for more details on the incident classification process.

### 3.1.2 Develop Incident Response Plan

- **Input:** Organizational Structure (Section 2.1.1), IACS Asset Classification (Section 2.1.2), Incident Classification (Section 2.2), Incident Response Team (Section 2.3), Monitoring IACS Environment (Section 2.5), Incident Response Policy (Section 2.4.1), Operational Cycle process (Section 2.4.3)
- **Action:** Develop IRPs for IACS cyber security incidents.
- **Output:** IRPs for IACS cyber security incidents.

**Implementation guidance:**

An IACS cyber security IRP aims to formally document the activities and procedures for handling all IACS cyber security incidents in an organization efficiently and adequately. The process owner should prepare the IRP with a clear goal for an incident response within a defined scope based on the cyber security incident response policy. The process owner would often collaborate with the IACS asset owners, subject matter experts, and managers to develop the IRP. The plans should be approved by senior management approval and be supported by them.

The plan includes the workflow of incident response activities to provide structure and pointers to the various response components. The following are examples of elements that should be included in an IRP:

- Mission;
- Strategies and goals;
- How the IRP fits into the overall organization;
- Senior management approval;
- Organizational environment and assigned incident response resources;
- The plan trigger events:
  - Monitoring, notification, and incident classification;
  - Incident Classification Guideline.
- CSIRT formulation guide;
- The approach to incident response;
- Escalation path;
- How the incident response team will communicate with the rest of the organization and external stakeholders;


https://t.me/learningnets

- Metrics for measuring the incident response tasks and their effectiveness;
- Roadmap for maturing the incident response capability:
  - IRP evaluation process;
  - IRP test and exercise process.

Refer to Section 2.4.2 for more details on IRP.

### 3.1.3 Test Incident Response Plan

- **Input:** Incident response policies (Section 2.4.1), IRPs (Section 2.4.2)
- **Action:** Develop and conduct incident response plan tests.
- **Output:** Completed incident response test, test results documented, lessons learned, IRP update.

**Implementation guidance:**

In order to execute an effective incident response, organizations should develop and conduct incident response plan tests on a regular basis. The frequency of the test should be determined in the established incident response policy. As an industry best practice, it is recommended that the test is performed once a year at a minimum. By testing and exercising the IRPs, the organization can evaluate and update the IRPs. In addition, this provides training to personnel in handling security incidents.

*NIST Special Publication 800-84* defines two types of exercises that can be conducted to test the incident response plan:

- **Tabletop Exercises:**
  Tabletop exercises are facilitated discussion-based exercises where personnel meet to discuss roles, responsibilities, coordination, and decision-making of a given scenario.
- **Functional Exercises:**
  Functional exercises allow personnel to validate their readiness for emergencies by performing their duties in a simulated environment.

When organizing an exercise, facilitators should take care to ensure that the invited participants come from a variety of areas / departments. Individuals that fill key roles must attend or send a delegate. Both types of exercises should allow personnel to go through each stage of incident response as guided by the IRP.

Prior to the exercise, facilitators should prepare the following:

- **A comprehensive exercise overview**
  The facilitator will use this overview to guide participants through the exercise. Key points and scenario developments should be detailed in this overview. Questions for participants can also be prepared in advance to point them in the right direction. A copy or summary of relevant IRPs should also be available.
- **A briefing for participants**
  The briefing informs the participants of the scenario constructed for the exercise. This can be delivered on paper or orally.

Following the completion of the exercise, the facilitator should author a lessons learned report. The main purpose of this report is to summarize where the participants excelled and what areas for improvement exist. It will also serve as evidence that the exercise was conducted.

Participants should be debriefed at the end of the scenario. In addition to providing them with feedback, the facilitator should also question the participants about their conclusions from the exercise. These questions can cover topics such as whether they feel confident in their ability to respond to an actual incident, whether they understand the roles and responsibilities of each CSIRT member, strengths / weaknesses identified during the exercise, etc.


https://t.me/learningnets

## 3.2 Incident Detection

### 3.2.1 Monitoring the IACS Environment

- **Input:** Classification of assets, controls, vulnerabilities, incident classification, IRP(s), acceptance incident response decisions, incident response related communications, and information about the IACS operational environment from internal and external sources.
- **Action:** Assets, cyber security controls, and vulnerabilities should be monitored and evaluated to identify any changes in the IACS environment and maintain an overview of the complete cyber security incident response posture.
- **Output:** Initiating incident response plan(s) by identifying incidents, communicating with stakeholders based on the level and type of incidents, or logging the identified event / incident.

**Implementation guidance:**

System monitoring is a crucial part of the incident response process that ensures abnormal system activities or events are detected in a timely manner. The faster an incident is detected, the sooner a response can be mounted, possibly reducing the potential impact. For further information on the general monitoring principles, refer to Section 2.5.

Incident indicators can come from various sources such as computer security software alerts, logs, publicly available information, and people. Table 8 lists common sources of indicators for each category.

**Table 8: Common Sources for Incident Indicators**

| Alerts | Description |
|---|---|
| Intrusion Detection and Prevention System (IDPS) | IDPS products monitor network activity for suspicious traffic and log important information. They can be used to identify types of attacks, source, and destination addresses, etc. |
| SIEM | Security Information and Event Management (SIEM) products analyze log files for key information. These products can be configured to identify certain behaviors and generate alerts accordingly (e.g., service failures). |
| Antivirus and antispam software | Antivirus software scans different types of files to detect malware. Its purpose is to prevent malware from infecting endpoints and alert appropriate personnel of the issue.<br>Antispam software automatically scans email messages to detect spam and reduce the potential for infection via user mistakes. |
| File integrity checking software | File integrity checking software watches important files for changes. Unexpected or unplanned changes to files can indicate a potential attack or a failure to follow change management procedures. |


https://t.me/learningnets

| Logs | Description |
|---|---|
| Operating system, service, and application logs | Log files generated by operating systems, services, and applications are one of the best resources for collecting evidence when an incident occurs. Organizations should develop a logging baseline for different systems. A higher logging level should be enforced for more critical systems. |
| Network device logs | Logs from network devices such as firewalls and routers can contain information about network traffic patterns, including blocked connection attempts. This information can be valuable in observing network trends and in correlating detected events from multiple devices over a network. |

### 3.2.2 Documenting Events / Incidents

- **Input:** The data from every single process, inter-process interactions, and information about the operational environment from internal and external sources.
- **Action:** Select portions of input data from all other processes that should be securely recorded and reliably available.
- **Output:** Feeding the documented data to the review and improvement process, incident analysis process, and the incident communication process.

**Implementation guidance:**

Incident management processes and their outputs should be documented through an appropriate mechanism. In this process, the scope and metrics of documentation are predefined. This mechanism should select some factors from the data generated by each process, which allows comprehension, investigation, analysis, and repetition of considerable events within that process or inter-process communications.

All events, changes, results, requirements, decisions, responses, effects, processes, and communications get recorded accordingly.

As the first step of incident response, the incident response team that suspects that an incident has occurred should immediately start recording all facts regarding the incident. Documenting system events, conversations, and observed changes in files can lead to a more efficient, more systematic, and less error-prone handling of the problem. Using an issue tracking system helps to ensure that incidents are handled and resolved in a timely manner. The issue tracking system should contain information on the following:

- The current status of the incident (new, in progress, forwarded for investigation, resolved);
- A summary of the incident;
- Indicators related to the incident;
- Other incidents related to this incident;
- Actions that are taken on this incident;
- Chain of custody, if applicable;
- Impact assessments related to the incident;
- Contact information for all involved parties (e.g., system owners);
- A list of evidence gathered during the incident investigation.

## 3.3 After Detection

### 3.3.1 Classify Incident

- **Input:** Incident records, asset profile, existing cyber controls profile, list of identified vulnerabilities, identified risks, Incident Classification Guide (Section 3.1.1).
- **Action:** The incident response process owner should classify incidents following the incident classification guideline.
- **Output:** Classification of the IACS cyber security incident.


https://t.me/learningnets

**Implementation guidance:**

The purpose of incident classification is to understand the type, source, scope, and impact of the cyber incident by investigating the incident records and reviewing the severity of the IACS cyber security incident.

The process owner would first collaborate with the asset owners or administrators to gather all appropriate incident information and then follow the Incident Classification Guide to classify the incident. The predefined Incident Classification Template, including the incident types, impact classes, and severity levels (Section 2.2), helps to have a standardized and expedited incident classification process.

### 3.3.2 Activate Incident Response Plans

- **Input:** IACS cyber security incident IRP(s) (Section 3.1.2), incident classification, and records of the incident that occurred.
- **Action:** The appropriate IRP activated and prioritization of actions should be identified and executed, stakeholders in the response plan should be notified, and immediate containment if needed (refer to Section 3.3.5.2), the Emergency Operation Center (EOC) selected if required.
- **Output:** Activate Incident Response Plan(s), incident communications, and potentially perform immediate containment actions.

**Implementation guidance:**

Activating the proper IRPs and prioritizing the activities to the incident is the most critical decision point in the incident handling process. Based on the scope and the classification of the incident, an appropriate IRP should be selected.

The process owner should prepare an IRP prior to the event, with a clear goal for an incident response within a defined scope based on the cyber security incident response policy. Please refer to Section 2.4.2 for a detailed description and scope of IRP.

The responsible Incident Commander (IC) gets assigned by the process owner based on the classification and scope of the incident. If applicable, the incident response process owner should also define roles and relationships with external CSIRTs.

The Incident Response Plans for large incidents would likely call for the activation of the Emergency Operation Center (EOC) site. To expedite the site selection process during an actual incident response, organizations should identify potential locations in advance. The Incident Commander should identify and select suitable EOC locations based on the type and complexity of the cyber security incident. Ideally, the EOC should be in a location that is easily accessible to CSIRT members and near the main IACS cyber security and network team.

### 3.3.3 Formulate CSIRT

- **Input:** Selected response plan, CSIRT formulation guide.
- **Action:** Identify the personnel that will fill the roles of the CSIRT according to the CSIRT formulation guide.
- **Output:** Selected CSIRT members are notified and mobilized.

**Implementation guidance:**

The initial preparatory work completed in Section 2.3.4 should be used to expedite this process. For example, a matrix such as the one presented in Table 6 makes it clear what level of management should become involved for each incident severity. As a reminder, the CSIRT roles are as follows:

- **Incident Commander (IC):**
  Leads and coordinates the overall incident response efforts
- **Public Information Officer:**
  Manages communications with internal and external stakeholders
- **Safety Officer:**
  Responsible for maintaining overall safety during the incident response process
- **Liaison Officer:**
  Manages communications with government agencies, regulatory authorities, and mutual aid partners during an incident.
- **Operations Section:**
  Responsible for performing the actual incident response plan implementation and reporting to the CSIRT on its progress. The operations section could also assist the Planning Section in developing an adequate incident response plan as subject matter experts.
- **Planning Section:**
  Responsible for planning the incident response process.


https://t.me/learningnets

- **Logistics Section:**
  Responsible for coordinating any additional human or material resources are required to perform the incident response activities.
- **Finance / Administration Section:**
  Responsible for ensuring that financial requirement is met to support the incident response activities.

It should be noted that the CSIRT does not need to be formulated all at once – certain roles may take priority and can be stood up before others. The team can be expanded or reduced as necessary to efficiently support incident response actions. CSIRT formulation can be re-evaluated in every Incident Operational Cycle (Section 2.4.3)

> For example, during initial incident analysis, the CSIRT may only consist of an IC and Operations Section. As the analysis is completed and the scope of the incident is determined, containment and eradication tasks are identified. These tasks are numerous and complex – managing the resources required to execute is beyond the capabilities of the IC. Therefore, the Planning, Logistics, and Finance Sections are stood up to assist. The severity of the incident requires that stakeholders be informed, so a Public Information Officer is assigned to handle those duties. As the incident concludes, the bulk of the containment, eradication, and recovery work has been completed. Consequently, there are fewer tasks to manage, and the Planning and Logistics Sections are stood down accordingly.

The expected recoverability effort should be considered when formulating the CSIRT roster. For example, the extended or prolonged incident response would require the assignment of multiple teams or roles that could rotate in shifts. Table 9 shows examples of recoverability effort categories that reflect the size and type of resources required to recover from the incident.

**Table 9: Incident Recoverability Effort**

| Resources Type | Description |
|---|---|
| Regular | Time to recovery is predictable with existing resources |
| Supplemented | Time to recovery is predictable with additional resources |
| Extended | Time to recovery is unpredictable; additional resources and outside help are needed |

### 3.3.4 Incident Communications

- **Input:** All incident information obtained from the incident management processes, including decisions, results, monitoring events, etc.
- **Action:** Continuous information about cyber security incident activities should be exchanged or shared between the CSIRT and other stakeholders.
- **Output:** Ongoing and comprehensive understanding of cyber security incident response objectives, decisions, plans, and results.

**Implementation guidance:**

Incident communication is a cyber security incident response activity that spans all incident activities in monitoring, assessment, response, post-incident processes. Incident communication is necessary to manage incidents as it facilitates information sharing between the CSIRT and other stakeholders. This information may include, but is not limited to:

- Characteristics of the cyber security incidents / events;
- Incident response plans, objectives, progress, and results;
- CSIRT formation;
- Incident containment processes and results;
- Incident eradication processes and results;
- Incident recovery processes and results.


https://t.me/learningnets

Effective communication between the CSIRT and stakeholders improves decision making and ensures that those responsible for implementing incident response activities understand the basis for these decisions.

Incident communication benefits incident response in the following ways:

- Informs responsibilities and enforces accountability for decision-makers and stakeholders;
- Collects incident information;
- Obtains new cyber security knowledge and sufficient oversight to support decision-making;
- Brings different areas of expertise together for each step of the incident response process;
- Coordinates with other parties and response plan to reduce consequences of any incident;
    - Coordinates operation of various incident response activities;
    - Gets help from experts and resources to mitigate or share cyber incidents / events.

The CSIRT would likely need to provide incident reporting to the upper management and various stakeholders throughout the incident response. The Public Information Officer (PIO) would be responsible for managing internal and external stakeholder communication. The parties that are typically notified include:

- Chief Information Officer;
- Head of cyber security;
- Local cyber security officer;
- Other incident response teams within the organization;
- Affected system owners;
- Public affairs (for incidents that may generate publicity);
- Legal department (for incidents with potential legal ramifications).

The Liaison Officer would manage communications with government agencies, regulatory authorities, and mutual aid partners during an incident.

The CSIRT should select the communication methods that are appropriate for a particular incident situation. Possible communication methods include:

- Email;
- Website (internal, external, or portal);
- Telephone calls;
- In-person.

The regularly occurring Operations Briefings provide information that the PIO and Liaison Officer can forward to various stakeholders. For complex incidents, the CSIRT may require legal or executive review and approval before information is released the public.

### 3.3.5 Response Stages

Once the initial incident response phase of incident notification, classification, IRP activation, and CSIRT formulation is completed, the incident response enters the response phase that consists of Analysis, Containment, Eradication, and Recovery stages. These response stages are organized and worked through in CSIRT using the Operational Cycle. The Operational Cycle ensures effective communications between the CSIRT members and promotes informed, collaborative decisions during the incident response. Refer to Section 2.4.3 for more detail on the Operational Cycle.

#### 3.3.5.1 Analysis

- **Input:** Incident records, classification, CSIRT, incident response plan, incident containment status, incident eradication status, incident recovery status.
- **Action:** Incident records should be thoroughly analyzed to ensure appropriate incident response actions are planned and executed. Align the incident action plan (IAP) and CSIRT accordingly, analyze the containment, eradication, and recovery status, align the response plan, CSIRT and make decisions accordingly.
- **Output:** Analysis of the incident, adjustment of IRP, CSIRT formulation update, incident containment plan, incident eradication plan, incident recovery plan, relevant communications.


https://t.me/learningnets

**Implementation guidance:**

Any incident response actions executed (Containment, Eradication, Recovery, or CSIRT formulation update) should be derived from thoughtfully planned actions made in the incident analysis step.

### Initial Analysis

At the start of a suspected incident, the CSIRT will perform an initial analysis. This analysis should be detailed enough to allow the CSIRT to accurately classify the incident and plan for appropriate follow-up actions. Key information that should be confirmed includes what systems are affected, the attack vector used, and the source of the incident. Detailed documentation of steps taken should be kept.

Time may be critical depending on the scope of the incident. Establishing a predefined process to follow will help expedite the completion of the initial analysis. The following recommendations may make initial analysis easier:

- **Maintain a baseline of networks and systems**
  Comparing current network and system behavior against this baseline will help identify anomalies, which may indicate an active incident.
- **Enforce log retention**
  Logs from firewalls, intrusion detection systems, servers, and other devices may provide insight into what transpired during an incident. Older logs may also help identify related incidents that preceded current events.
- **Identify related events.**
  By correlating information from different sources (e.g., event logs, system monitoring tools), the CSIRT can gain a more comprehensive view of the overall situation. A sequence of events can also be determined. For this to be possible, all devices must be time synced to the same source.
- **Collect additional data using a passive traffic sniffer.**
  Sometimes the indicators do not record enough details to understand the nature and scope of the incident. If an incident is occurring over a network of devices, having a packet sniffer to capture network traffic is one of the fastest ways to collect the necessary data.
- **Seek Assistance from Others.**
  Occasionally, the CSIRT won't be able to determine the full cause and nature of a cyber incident. If the CSIRT lacks sufficient information to analyze, contain, eradicate and recover from the incident, then they should consult with internal and / or external resources.

### Containment Analysis

Containment is required for the majority of incidents, so it is crucial to act quickly in handling each cyber incident. Containment assures non-spreading of the incident and buys time for developing a remediation strategy. Decision-making is very important in initiating the containment process and choosing containment activities. Having predetermined procedures for containing incidents facilitates faster and more effective decision-making.

Based on predetermined strategies or tabletop exercises, and by reviewing the incident records, the CSIRT decides whether the containment process is needed or not. The CSIRT defines the containment goals and measures.

After a cycle of containment process, if needed, CSIRT analyzes the results of the containment process and validates them with the defined goals and measures. If the containment goals are not achieved, either another cycle of containment process is initiated, or new containment goals and measures are defined.

### Eradication Analysis

Once containment is complete, eradication efforts can begin to permanently remove attackers from the network environment. To achieve this, identified attack vectors are mitigated, and vulnerabilities are addressed so that the same attack or the same class of attack will be prevented.

Some eradication activities should be performed in conjunction with recovery. For example, if a virtual machine is reimaged, it should also be hardened after recovery is complete so that it cannot be compromised through the previously used attack vector.

By reviewing the incident records, the CSIRT decides whether the eradication process is needed or not. CSIRT defines the containment goals and measures.

After a cycle of the eradication process, if needed, CSIRT analyzes the results of the eradication process and validates them with the defined goals and measures. If the eradication goals are not achieved, either another cycle of the eradication process is initiated, or new eradication goals and measures are defined.

### Recovery Analysis

If the analysis shows that any system is not operating normally, the recovery process needs to be initiated. CSIRT defines the normal operation goals and measures


https://t.me/learningnets

for systems and initiates the recovery process. Typically, the goal of the recovery process is to bring the operation of systems back to as they were before the incident. However, this may change according to the outcome of the eradication process.

> CSIRT will advise and request the system operations or owners about the time of returning to service. The system owners would make the final decision on the return time.

CSIRT, in collaboration with system owners, decides on the latest backup / images that are clean and can be trusted.

CSIRT and system owners agree on measures to test, monitor, and verify that the system is back fully operational and clean.

After a cycle of the recovery process, if needed, CSIRT analyzes the results of the recovery process and validates them with the defined goals and measures. If the recovery goals are not achieved and / or normal operation tests fail, either another cycle of the recovery process is initiated, or new recovery goals and measures are defined.

**CSIRT Formulation Analysis**

CSIRT continuously evolves throughout the incident response. CSIRT formulation could be re-evaluated in every incident Operational Cycle (Section 2.4.3) to ensure adequate resources are assigned to support incident response actions efficiently. The CSIRT could be expanded or reduced depending on the stage and the scope of the incident response. For example, if the cyber security incident becomes more severe by compromising the larger scope of IACS assets, CSIRT should be expanded to support the incident growth. On the contrary, towards the end of the Recovery phase, some CSIRT members can be dismissed to go back to their regular roles and responsibilities. The Logistics Section would be responsible for recruiting or dismissing appropriate CSIRT members throughout the process.

### 3.3.5.2 Containment

- **Input:** Decision on whether containment is required, evidence from monitoring, network diagrams, asset profiles, containment goals, and measures.
- **Action:** Determine and execute the appropriate actions to contain the cyber security incident.
- **Output:** Containment methods employed, containment status report.

**Implementation guidance:**

The purpose of containment is to limit the scope of actual or potential damage and prevent the incident from spreading. For cyber security incidents, this typically involves identifying affected systems and isolating them.

Before incidents occur, the organization should develop containment strategies for various incident types. For example, the strategy for containing an email-borne malware infection differs greatly from malicious disruption of backup systems. For each major incident type, containment strategies should be developed with criteria documented clearly to facilitate decision-making. Criteria for determining the appropriate strategy may include:

- Potential damage to resources;
- Need for evidence preservation;
- Service availability;
- Time and resources needed to implement the strategy;
- Effectiveness of the strategy;
- Duration of the solution.

Before performing containment activities, ensure that all relevant stakeholders are informed of the actions taken – maintaining communication during this process is critical. It is important to remember that isolation of IACS may impact Operations and Safety.

Containment of devices can be established in two ways: physically and logically. A combination of the two methods can also be used.

Physical containment involves disconnecting the affected devices from the network by de-powering them and / or disconnecting communication interfaces. Care should also be taken to secure any out-of-band management methods. Proper physical containment guarantees that the disconnected devices are entirely separate from the rest of the network. However, this approach is not always viable and may affect the network and IACS


https://t.me/learningnets

in unexpected ways. The recovery phase may also be hindered if the physical containment methods employed were not well documented.

Logical containment is typically easier and faster to accomplish, as the affected devices can be isolated by reconfiguring networking devices, firewalls, etc. However, it is more difficult to ensure that the implementation is secure, given that a compromised networking device could potentially circumvent the established perimeter.

Ideally, only the affected sections of the network will be isolated. Depending on the type and severity of the incident, the decision may be made to sever all connections between the IT and OT sides of the corporate network. Where full isolation is not possible or practical, hardening the affected systems should be done before eradication. All containment actions performed should be documented, as many measures will need to be removed during the recovery phase.

If the cyber security incident analysis results indicate that the situation is severe, immediate containment actions may be warranted. In such situations, severing the connection between the IT and OT networks is strongly recommended – a simpler mandate like this requires less time to implement than the effort needed to pinpoint the affected network segments. For the same reason, physical containment methods are also recommended – they are less prone to error and are easier to verify.

> Sometimes the attacker can be redirected to a sandbox to monitor their activity, usually to gather additional evidence. Monitoring an attacker should only happen when the compromised systems are isolated and do not allow the compromise to continue; otherwise, the CSIRT may be liable if the attacker uses the compromised system to attack other systems. Consider the risk of delaying the containment, as the attacker could escalate unauthorized access or compromise other systems. CSIRT should not assume that just by isolating a host, further damage to the host has been prevented.

During or after the containment process, it is prudent to capture a snapshot of the current state of each device. This snapshot can be used as evidence in subsequent forensic analysis and may also be helpful in recovery.

Compromised user, service, and administrator accounts also need to be addressed, as they can traverse the network. Affected accounts should be locked down and disabled. Some of these accounts may be critical to the operation of some processes or services – the effects should be known before disabling these accounts to mitigate any adverse impacts to Operations or Safety.

The appropriate personnel to perform the task must be determined. For example, depending on the organization's structure, a team or individual from the Operations Section may be suitable, or other IT resources may be brought in to supplement the CSIRT.

### 3.3.5.3 Eradication

- **Input:** Incident Analysis decision on eradication plan, eradication goals, and measures.
- **Action:** Complete the appropriate actions to eliminate the cause of the cyber security incident.
- **Output:** The cause of the cyber security incident is eradiated, system hardened to the normal baseline, eradication status report.

**Implementation guidance:**

Monitoring data should be analyzed to determine the attacker's method to exploit vulnerabilities to gain access, escalate privileges, and traverse the network. A typical goal of eradication is to fix vulnerabilities and prevent attackers from performing similar attacks. These vulnerabilities may be addressed using methods that include, but are not limited to:

- Defining new firewall rules.
- Hardening of devices through limiting of ports and services, uninstalling unnecessary software, etc. If available, hardening checklists can be used to aid in this process.
- Performing software or firmware updates. Applicable security patches and hotfixes should also be applied.

A skilled attacker will introduce backdoors into the system to secure their access. If a backdoor is not removed, the assailant will regain entry to the network with ease. Therefore, it may be prudent to reset devices to their factory default settings or another known, clean state. In cases where the device cannot be reset or reimaged, eradication will have to be performed manually or a suitable antivirus software employed.

The eradication plan made in Incident Analysis would be executed cautiously and thoughtfully. It is recommended that the system be continuously monitored to ensure no unexpected errors or system abnormality occurs. If any unexpected results are observed, the Operations team should stop the eradication actions and contact the Planning team for further incident analysis. All actions taken during this phase should be thoroughly documented.


https://t.me/learningnets

#### 3.3.5.4 Recovery

- **Input:** Incident Analysis decision that recovery actions are required, recovery goals and measures.
- **Action:** Conduct the appropriate actions to restore and return affected systems and devices back to the desired state of operations.
- **Output:** Components of the affected system fully restored, recovery status report.

**Implementation guidance:**

The goal of the recovery phase is to restore and return the affected systems and devices back to the desired state defined in the analysis phase. The recovery goal and normal operation testing measures are defined as the input of this process.

The recovery actions must be completed cautiously and thoughtfully to avoid another incident from occurring. It is critical to test, monitor, and validate the systems by components or phases to minimize the risk of re-infection or re-compromise of the system. If any unexpected results are observed, the Operations team should stop the recovery actions and contact the Planning team to analyze further. All actions taken during this phase should be thoroughly documented.

Considering the advice of CSIRT, system owners decide how to test, monitor, and verify that the system is back fully operational and clean. This includes monitoring the system for an amount of time to validate that there is no further re-infection or re-compromise and the tools to test, monitor, and validate the systems.

## 3.4 Post-Incident

### 3.4.1 Review and Improvement

- **Input:** Incident classification and records, communications, ongoing progress status, final reports for all incident response processes, executed tasks, and activities, and information about the operational environment from internal and external sources.
- **Action:** Procedures, actions, measurements, expectations, communications, deliveries, monitoring, documentation, evaluations, and decision-making processes should be reviewed to improve or maintain them.
- **Output:** Updating of incident response plan components, responsibilities, requirements, procedures, controls or tools, lessons learned document.

**Implementation guidance:**

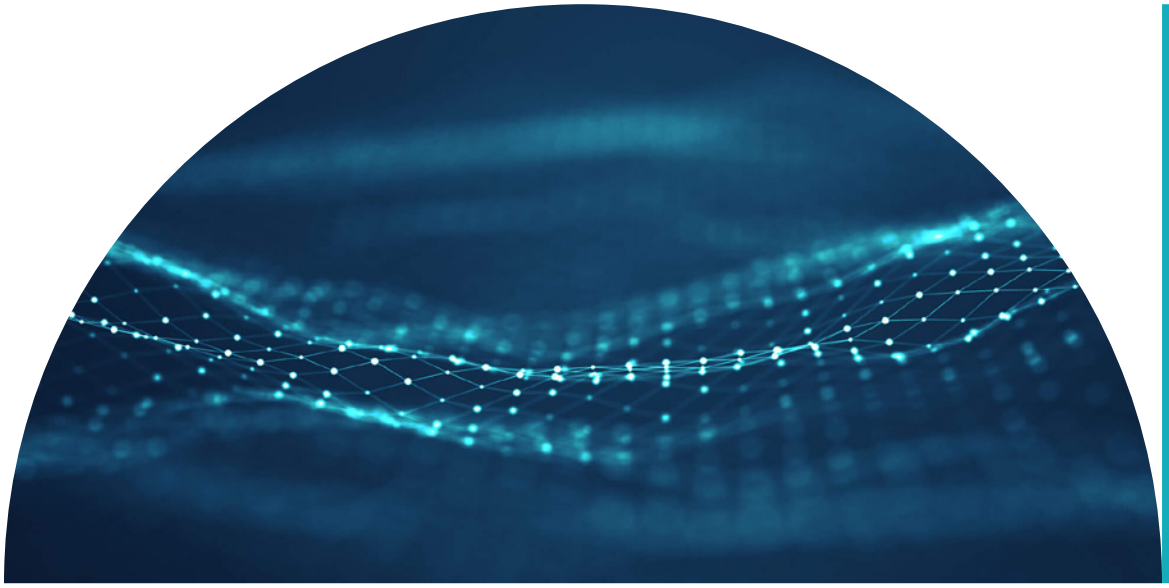
Once the incident response actions are completed and the system is fully recovered, the CSIRT should hold a post-incident review session. This meeting aims to review all the evaluations, plans, decisions, communications, and actions made during the incident response. Lessons learned should be identified to improve the overall effectiveness and efficiency of the incident response process and to ensure that current practices align well with the business objectives, strategies, and policies.

Factors that may be considered during review and improvement include, but are not limited to:

- Communication methods;
- Incident assessment and classification methodologies;
- CSIRT formulation method;
- Cyber security culture and/or awareness;
- System monitoring strategies;
- Containment strategies;
- Backup and recovery strategies.

All improvements to the process should be reflected in the IRP, and process owners and managers should be notified. Moreover, the organization should ensure that incident response resources are always available to review incidents, address new threats / vulnerabilities, and advise management accordingly.


https://t.me/learningnets



CHAPTER 4

# References


[1] «NIST Special Publication 800-61 - Computer Security Incident Handling Guide,» National Institute of Standards and Technology, 2012.

[2] «NIST Special Publication 800-82 - Guide to Industrial Control Systems (ICS) Security,» National Institute of Standards and Technology, 2015.

[3] «NIST Special Publication 800-39, managing information security risk: Organization, mission, and information system view,» National Institute of Standards and Technology, 2011.

[4] BBA, «IACS Cybersecurity Risk Methodology,» https://www.bba.ca/expertise/industrial-cybersecurity/, 2020.

[5] «MITRE Partnership Network,» [Online]. Available: https://collaborate.mitre.org/attackics/index.php/Main_Page.

[6] «CSA Z1002: Occupational health and safety - Hazard identification and elimination and risk assessment and control,» CSA, 2017.

[7] «Open Risk Analysis Technical Standard (O-RA),» The Open Group, 2013.




https://t.me/learningnets

[8] «ISO/IEC 27005 - Information Security Risk Management,» International Organization for Standardization, 2018.

[9] «NIST Special Publication 800-30 - Guide for Conducting Risk Assessment,» National Institute of Standards and Technology, 2012.

[10] «ISO 31010: Risk Management - Risk Assessment Techniques,» International Organization for Standardization, 2019.

[11] «ISA-62433-3-2 Security Risk Assessment and System Design,» International Society of Automation, 2018.

[12] «ISO 31000: Risk Management - Guidelines,» International Organization for Standardization, 2018.

[13] ICS Canada, «ICS Canada,» 2012. [Online]. Available: http://www.icscanada.ca/images/upload//ICS%20OPS%20Description2012.pdf.

[14] «ISO/IEC 27035-2 - Information Security Incident Management,» International Organization for Standardization, 2016.

[15] «Developing an Operational Technology and InformationTechnology Incident Response Plan,» Public Safety Canada, 2020.

[16] «The Incident Handlers Handbook,» SANS Institute, 2011.

[17] «ICS 100 - Introduction to the Incident Command System,» FEMA Emergency Management Institute, 2018.

[18] «https://www.icscanada.ca/en/about+ics+canada.html» [Online].



https://t.me/learningnets

APPENDIX A

# Glossary

**Asset Security Zoning.** The physical and logical grouping of the cyber assets with similar cyber security requirements.

**Attack Vector.** The path(s) or means by which an attacker can make the cyber security attack happen.

**Cyber Asset.** A programmable electronic device, including the hardware, software, and data in the device.

**Cyber Security Control.** An action, tool, procedure, or technique that reduces a cyber threat, vulnerability or attack, by reducing the harm it can cause or by increasing visibility over cyber incidents in order to take corrective actions.

**Cyber Security Event.** Events with negative impacts to a computer system, such as execution of malware or virus, loss of network connection, and storage drive failure.

**Cyber Security Incident.** "An occurrence that results in actual or potential jeopardy to the [safety, reliability,] confidentiality, integrity or availability of the information, the system processes, stores, or transmits or that constitutes [an]…imminent threat of violation of security policies, security procedures, or acceptable use policies" [1].

**Cyber Security Incident Response Policy.** See *Incident Response Plan (IRP).*

**Cyber Security Incident Response Team (CSIRT).** A team assembled to assess, contain, eradicate, and recover from a cyber security incident.

**Impact.** The magnitude of harm that can be expected to result from consequences of cyber security violations by a variety of organizational and non-organizational stakeholders.

**Incident Command System (ICS).** A standardized emergency management system designed to provide robust and efficient incident management by effectively coordinating facilities, equipment, personnel, procedures, and communications within an organization.

**Information Technology (IT).** Communication and computing devices that are not involved with the control of physical processes. Typically refers to an organization's corporate network.


https://t.me/learningnets

**Incident Action Plan (IAP).** A written plan containing objectives, action items, and execution directions for managing incident response.

**Incident Commander (IC).** The individual responsible for managing a cyber security incident, maintaining safety during the incident, providing information services to internal and external stakeholders, and coordinating with other participating agencies

**Incident Response Plan (IRP).** A written plan that supports the response to a security incident in a systematic, proactive, and efficient manner.

**Incident Response Process Owner.** The individual responsible for overseeing the planning, preparation, and execution of incident management activities based on the cyber security incident management policy and Incident Response Plan(s).

**Industrial Automation and Control Systems (IACS).** Refers to Programmable Logic Controllers, Distributed Control Systems, Safety Instrumented Systems, and other associated devices that enable communication between these devices. Together, these computing systems are used to control physical processes.

**Intrusion Detection Systems (IDS).** Monitors network traffic for unusual behavior which may be indications of a cyber security incident. This device is passive.

**Intrusion Prevention Systems (IPS).** Monitors network traffic for unusual behavior which may be indications of a cyber security incident. This device is also capable of acting to mitigate detected cyber security incidents by severing connections, blocking traffic, etc.

**Operational Cycle.** A cyclical process that consists of establishing objectives, execution tactics, plans, and briefings to ensure that an adequate Incident Action Plan (IAP) is developed and executed. Each cycle is referred to as an **Operational Period**.

**Operational Technology (OT).** See *Industrial Automation and Control Systems. Often contrasted with Information Technology.*

**Risk.** A function of the likelihood of a threat event's occurrence and potential adverse impact when the event occurs. This broad definition also allows risk to be represented as a single value or as a vector of values, where different types of impacts are considered separately. In this definition of risk, all the above risk factors are involved.

**Risks can be grouped into some categories based on a combination of the risk factors.** The most popular way to categorize risks is based on impact categories. Some typical high-level categories of risks based on impact are financial, reputational, legal, safety, and environmental.

**Security Information and Event Management (SIEM).** Analyzes log files to detect potential cybersecurity events.

**Threat.** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), assets, IACS, individuals, other organizations or the community through an information, automation, monitoring or control system via intentional or unintentional unauthorized access, destruction, disclosure of information, modification of information or decision flow, malfunction, modification of workload or control path or denial of service.

**Vulnerability.** A weakness that can potentially be exploited. In cyber security, a vulnerability could be utilized to cause a cyber security event or incident.


https://t.me/learningnets

At BBA, we have a clear understanding of your challenges and objectives. Our presence in the field and natural curiosity to keep an eye on the latest technology allow us to fully comprehend your operations. We are here to help you make the right choices in building profitable and environmentally-friendly projects.

BBA.CA

https://t.me/learningnets