Your Logo
Will Be
Placed Here

INTEGRATED INCIDENT RESPONSE PROGRAM (IIRP)

ACME Business Consulting, LLC

IIRP
Integrated Incident
Response Program

INTERNAL USE
Access Limited to Internal Use Only

IT IS PROHIBITED TO DISCLOSE THIS DOCUMENT TO THIRD-PARTIES WITHOUT AN EXECUTED NON-DISCLOSURE AGREEMENT (NDA)

NOTICE

REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

This document references numerous leading industry frameworks in an effort to provide a comprehensive and holistic approach to identifying, detecting and responding to cybersecurity and privacy incidents. The following external content is referenced by or supports this Integrated Incident Response Program (IIRP) document:

- National Institute of Standards and Technology (**NIST**): [1]
  - NIST 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST SP 800-61: *Computer Security Incident Handling Guide*[2]
  - NIST 800-83: *Revision 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops*
  - NIST SP 800-86: *Guide to Integrating Forensic Techniques into Incident Response*[3]
  - NIST 800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
  - NIST 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
  - NIST 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
  - NIST *Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)
- International Organization for Standardization (**ISO**):[4]
  - ISO 27002: *Information Technology -- Security Techniques -- Code of Practice for Cybersecurity Controls*
  - ISO 27035: *Information Technology - Security techniques - Information Security Incident Management*
- Secure Controls Framework (SCF) [5]
  - SCF Security & Privacy Capability Maturity Model (SP-CMM)
  - SCF Privacy Management Principles
- Carnegie Mellon University Software Engineering Institute (CMU SEI)
  - An Introduction to the Mission Risk Diagnostic for Incident Management Capabilities (MRD-IMC)[6]
  - Building an Incident Management Body of Knowledge[7]
  - Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ)[8]
  - First Responders Guide to Computer Forensics: Advanced Topics[9]
  - Handbook for Computer Security Incident Response Teams (CSIRTs)[10]
  - Incident Management Capability Assessment[11]
  - Organizational Models for Computer Security Incident Response Teams (CSIRTs)[12]
  - State of the Practice of Computer Security Incident Response Teams[13]
- Other Frameworks:
  - Center for Internet Security (**CIS**)[14]
  - European Union Regulation 2016/279 (General Data Protection Regulation (**EU GDPR**))[15]
  - Payment Card Industry Data Security Standard (**PCI DSS**)[16]

[1] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[2] NIST 800-61 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[3] NIST 800-86 - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
[4] International Organization for Standardization - https://www.iso.org
[5] Secure Controls Framework - https://www.securecontrolsframework.com
[6] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91452
[7] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=53076
[8] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485652
[9] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7261
[10] https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf
[11] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538848
[12] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6295
[13] https://resources.sei.cmu.edu/asset_files/TechnicalReport/2003_005_001_14204.pdf
[14] Center for Internet Security - https://www.cisecurity.org/
[15] EU General Data Protection Regulation - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[16] Payment Card Industry Security Standards Council - https://www.pcisecuritystandards.org/

Table of Contents

Integrated Incident Response Program (IIRP) Overview

Introduction

The Integrated Incident Response Program (IIRP) is used as the guideline for managing cybersecurity alerts and events. This document provides an overview of ACME's corporate-wide incident response process.

Having one standardized framework provides a number of benefits, including:

- Increased protection of core business functionality, capabilities, and revenue generating systems;
- Reduced potential impact of non-remediated threats and vulnerabilities;
- Reduced potential impact of incidents to the brand, shareholders, customers, and business partners; and
- Ability to leverage a standardized, documented processes across the enterprise.

Scope & Applicability

The IIRP enables ACME employees to respond to cybersecurity incidents and restore normal operations as quickly as possible, while minimizing the adverse impact on business operations. This process and methodology ensures that the best possible levels of service quality and availability are maintained.

The scope of the framework includes all stakeholders in any incident response. The different Business Units (BUs), service providers, and applicable ACME subsidiaries are contained in the breadth of this document.

Assumptions

The following are assumptions related to the IIRP described in this document:

- ACME's cybersecurity policies and standards are communicated to and are followed by ACME's users, partners, and service providers.
- BUs respond to incidents by repeatable, internal processes that support the IIRP for the escalation and governance of incidents.

Alignment With Leading Practices

ACME's methodology used to respond to incidents is primarily based on the following National Institute of Standards and Technology (NIST) guidance:

- NIST SP 800-61, Computer Security Incident Handling Guide[17]
- NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response[18]

Key Terminology

The accepted definitions for cybersecurity terms shall be based on the NIST IR 7298, *Glossary of Key Information Security Terms*.[19] Highlighted below are key cybersecurity-specific terms that the reader of this document must be familiar with. Additionally, further cybersecurity-specific definitions can be found in the Glossary.

Asset. Any information system, peripheral hardware, application or data that is used in the course of business activities.

Event. Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. Examples of events include, but are not limited to:

- Event log entry (e.g., system/security/application);
- Security Incident Event Manager (SIEM) notification;
- Conversation (e.g., in person/email/phone/fax/IM);

[17] NIST 800-61 - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[18] NIST 800-86 - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

[19] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

- Service desk ticket; and
- Observation by an individual.

Incident. An assessed occurrence that actually or potentially jeopardizes:

- The confidentiality, integrity, or availability of an asset; or
- The data that an asset processes, stores, or transmits.

Examples of incidents include, but are not limited to:

- Lost/stolen asset;
- Malware outbreak; and
- Information security policy violation (e.g., violating acceptable use)

Integrated Security Incident Response Team (ISIRT). An ISIRT is a group of individuals who are organized to develop, coordinate and execute actions for the containment, eradication, and recovery resulting from cybersecurity incidents.

UPDATES

Updates to the IIRP will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes.

IIRP Structure

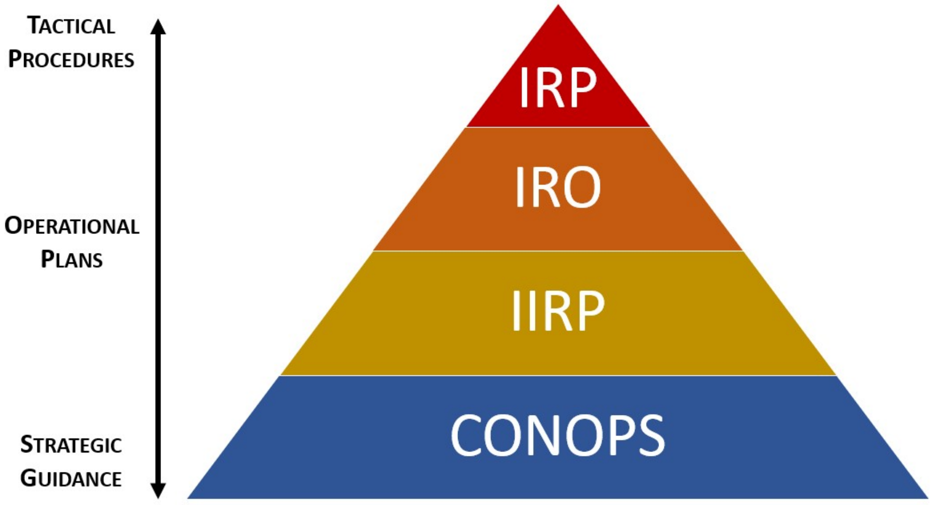
Incidents do not care if responders are or are not prepared to respond. What matters is appropriate leadership that is capable of directing response operations in an efficient and effective manner.

Hierarchical Approach To Incident Response

In order to implement an efficient and repeatable incident response methodology, it requires a structure that addresses the scope from a strategic to a tactical level.

At ACME, there are four (4) hierarchical components that define the concept of incident response across the enterprise:

- Concept of Operations (CONOPS)
- Integrated Incident Response Program (IIRP)
- Incident Response Operations (IRO)
- Incident Response Plan (IRP)



Concept of Operations (CONOPS)

ACME's policies and standards associated with incident response establish the strategic approach to incident response. This high-level corporate guidance forms ACME’s **Concept of Operations (CONOPS)** for incident response across the enterprise. This CONOPS helps communicate the quantitative and qualitative expectations to all stakeholders of what must be employed to achieve the desired objectives.

Integrated Incident Response Program (IIRP)

ACME’s **Integrated Incident Response Program (IIRP)** establishes the operational approach to addressing cybersecurity incidents, so that operations may be conducted in a proactive and sustainable manner.

The IIRP defines how ACME teams will work together to respond to an incident. It leverages ACME’s incident response capabilities to efficiently and effectively manage all levels of incident response. This allows for differing business units within ACME to “plug in” to organization-wide processes for responding to cybersecurity events and incidents.

The IIRP is an adaptable framework that:

- Is applicable for use across the enterprise;
- Provides a methodology to categorize incidents, assign severity and impact ratings;
- Assigns roles and responsibilities associated with incident response; and
- Breaks down incident response into manageable phases for escalating incidents and bringing groups together to respond to incidents.

The IIRP is not:

- A detailed Incident Response Plan (IRP) for use by business units or key stakeholders. (reference Annex 1: Incident Response Playbook for scenario-based incident response)

Incident Response Operations (IRO)

The IIRP calls out operational responsibilities for key stakeholders. When a stakeholder is engaged in the incident response process, those personnel are executing **Incident Response Operations (IROs)**.

With or without vetted IRPs, stakeholders are still responsible for responding to the incidents in a professional manner. A useful analogy is the childhood game of "hide and seek" where the game begins once the words "ready or not, here I come" are spoken. Incident response is very similar, since ready or not, the responder has to act. The better prepared the responder is, the more efficient the IRO will be. This preparation most often comes through documented IRPs and incident response exercises / training.

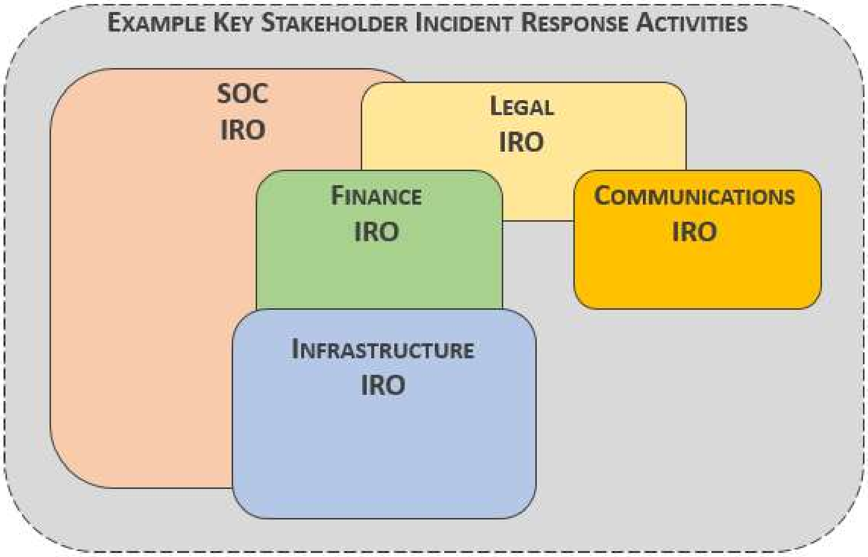
In order for incident response activities operate in an efficient and controlled manner at the stakeholder-level, IROs are expected to leverage **Incident Response Plans (IRPs)**. However, a stakeholder can still conduct IROs without an IRP. The downside to executing IROs without an IRP is that activities are ad hoc in nature.

IROs are simply areas of responsibility that are assigned to key stakeholders related to cybersecurity incidents:

- Every key stakeholder (e.g., department or team) involved in incident response has an IRO;
- Regardless if a participant is or is not prepared, that key stakeholder must respond in a professional manner to address the realities of the incident; and
- IROs may overlap and have areas of shared responsibility, so it requires teamwork and leadership involvement to ensure coordination is performed and tasks are completed.

In the example shown below, an incident may involve dedicated actions by several departments:

- Security Operations Center (SOC);
- Legal;
- Finance;
- Communications; and
- Infrastructure (e.g., firewall and database experts).



Each of these key stakeholders has a unique set of skills and areas of responsibilities. As shown in the diagram, some areas may overlap, but other areas are specific to their unique job functions at ACME. What makes these department-level IROs efficient is having well thought out and documented IRPs.

Incident Response Plans (IRPs)

At the department and/or team level, <u>IRPs establish the tactical-level approach towards incident response</u>. IRPs are:

- Meant to be tested and validated on a recurring basis to ensure applicability; and
- "Playbooks" that incident responders follow to ensure proper procedures are adhered to.

Incident responders should use IRPs to handle their response steps. An IRP is the tool that allows an IRO to have a repeatable structure, since IRPs can be tested to validate the effectiveness of the process(es):

- <u>Without an IRP, IROs operate in an ad-hoc manner</u>;
- IRPs provide repeatable, testable processes to conduct IRO responsibilities;
- IRPs should cover all reasonably-expected incident response scenarios;
- IRPs should be flexible enough to adapt to incidents, but be granular enough to guide an incident responder; and
- IRPs are a way to proactively answer certain incident responder questions:
  - What are the roles & responsibilities within my group?
  - What do I do when an incident happens?
  - Who do I contact?
  - When do I contact others?
  - How do I capture documentation?

Incident Response Phases

The IIRP addresses the high-level workflow from event collection, to incident declaration, to incident closure. The process flow framework, illustrated below, outlines the incident response phases:

Pre-Incident

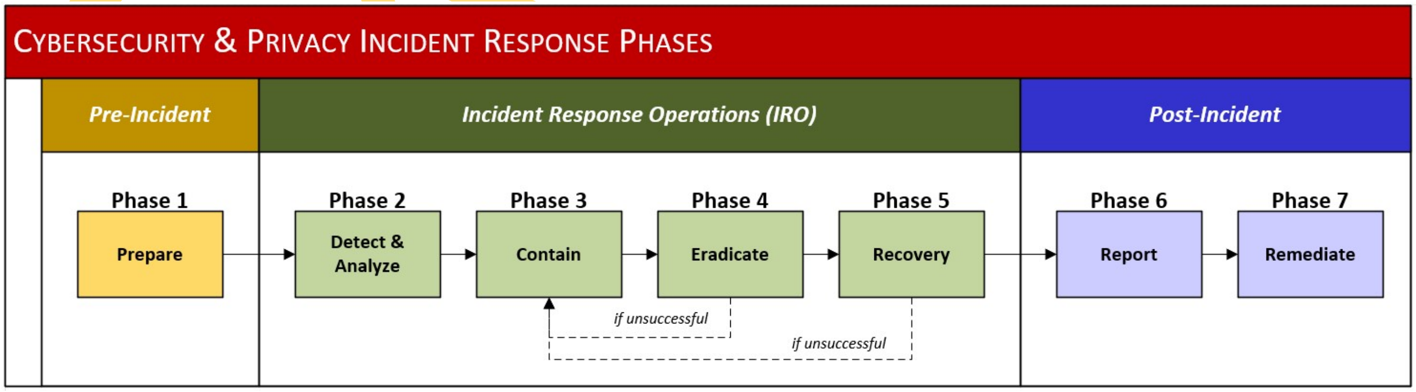
- Phase 1: Prepare

Incident Response Operations (IRO)

- Phase 2: Detect & Analyze
- Phase 3: Contain
- Phase 4: Eradicate
- Phase 5: Recovery

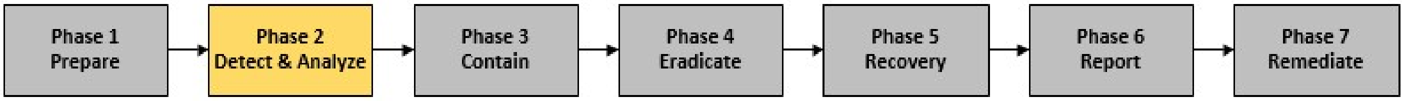
Post-Incident

- Phase 6: Report
- Phase 7: Remediate



PHASE 2 – DETECT & ANALYZE

The second phase is "Detect & Analyze" and these activities focus on identifying the type, severity and escalation of the cybersecurity incident.



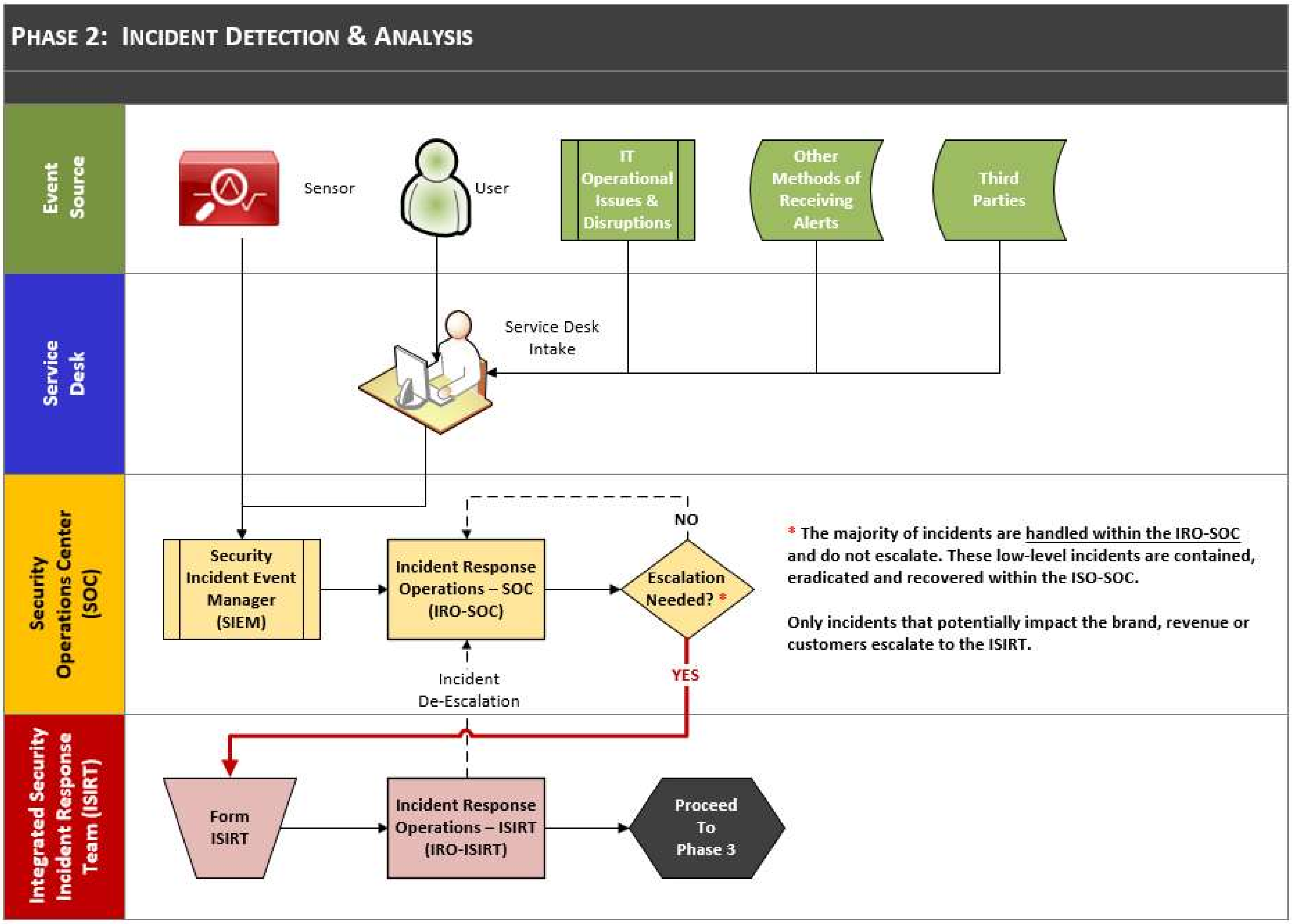
INPUTS

During the preparation phase, specific documentation enables the efficient execution of the follow-on phases of the IIRP process. This documentation includes:

- High Value Assets (HVA) list;
- High Value Data (HVD) map;
- Assigned incident response roles & responsibilities;
- Established contact lists; and
- Incident Response Plans (IRP).

WORKFLOW – DETECTION & ANALYSIS PROCESS

Before an incident can be analyzed and prioritized, the event in question must first be identified and an alert generated to notify the appropriate individuals.



PHASE 2: INCIDENT DETECTION & ANALYSIS
Event Source
Service Desk
Security Operations Center (SOC)
Integrated Security Incident Response Team (ISIRT)
Sensor
User
IT Operational Issues & Disruptions
Other Methods of Receiving Alerts
Third Parties
Service Desk Intake
Security Incident Event Manager (SIEM)
Incident Response Operations – SOC (IRO-SOC)
NO
Escalation Needed? *
YES
Incident De-Escalation
Form ISIRT
Incident Response Operations – ISIRT (IRO-ISIRT)
Proceed To Phase 3

* The majority of incidents are handled within the IRO-SOC and do not escalate. These low-level incidents are contained, eradicated and recovered within the ISO-SOC.

Only incidents that potentially impact the brand, revenue or customers escalate to the ISIRT.

Cybersecurity Department (CSD) Activities

CSD personnel are the key element in the initial assessment of events and determining what additional actions are required, if any. The general concept of CSD operations in this phase include:

- Automated Alert Notification Process. CSD will serve as intake and also receives automatic notification of incoming incidents. Once notified, it is their responsibility to escalate the incident appropriately.
- Incident Response Operations-CSD (IRO-CSD). Upon receiving the incident alert, CSD personnel will follow their own internal processes to validate and prioritize the potential incident. This may include reaching out to other teams to gather background information.

Business Unit (BU) Activities

The Business Unit (BU) is the business function or department within ACME that was affected by the cybersecurity incident. The BU operations in this phase include:

- Provide Details and Triage. The BU often has the greatest subject matter expertise of the cybersecurity incident and, because of this, will need to work with CSD to provide the details. The BU may also have a refined and mature process for handling cybersecurity incidents. If this is the case, the BU will provide an extremely active role in technical triage for the cybersecurity incident.
- Validate Risk Assessment and ISIRT Formation. The decision to create the ISIRT is ultimately done by CSD, but consensus from the BU is highly encouraged and enables effective incident response.

Integrated Security Incident Response Team (ISIRT) Activities

The general concept of ISIRT operations in this phase include:

- ISIRT Formed. Based on the type of incident and the involved parties, CSD and the BPL will identify the appropriate incident responders to participate in the ISIRT. Each member of the ISIRT is contacted and the team is established.
- Incident Response Operations (IRO) – ISIRT. Once the ISIRT is formed, the ISIRT Leader will direct work. At this point, Phase 2 ends and Phase 3 begins.

Incident Analysis

Determining whether a particular event is actually an incident is a matter of judgment, based on available facts. The incident responders should work quickly to analyze and validate event activities. When an incident responder believes that an incident has occurred, the incident responder should rapidly perform an initial analysis to determine:

- The incident's scope, such as which networks, systems, or applications are affected;
- Who or what originated the incident; and
- How the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited).

Incident Source Identification

Incident precursors and indications can come from both technical and human sources. The event source is simply the origin of the event. This can be either a human or technical source:

- System User. A user can identify a situation and report that issue to the Service Desk. This submission may be over the phone or via email.
- System-Generated Alert. Systems logging to the log aggregator (e.g., Security Incident Even Manager (SIEM)) will forward specific events without human interaction.
- Business Unit Personnel. Employees from a business unit can contact CSD directly about incidents.
- CSD Personnel. CSD may observe an alert or behavior that requires additional investigation. CSD personnel would be responsible for either opening a ticket with Service Desk or manually generating an incident ticket.
- ACME Leadership. Organization leadership may become aware of an event or incident that requires additional investigation. These organizational leaders are responsible for either opening a ticket with Service Desk or directly contacting CSD to open an investigation into the potential incident.

Evidence Analysis

Evidence analysis is a process in which evidence related to an incident is analyzed to learn more about it. While some evidence may provide all the information an incident responder might need with a surface examination, often, the evidence needs to be explored more deeply:

- The analysis process must be conducted by an incident responder who is experienced in proper techniques used to analyze and handle evidence, in order to ensure that evidence is not compromised during the analysis process.
- Incident responders should assume that an incident is occurring until they have determined that it is not. When in doubt, incident responders should assume the worst until additional analysis indicates otherwise.
- The initial analysis should provide enough information for CSD to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

Evidence-based technical analysis is the process used by ACME to apply the scientific method. Appendix C: Scientific Method of Evidence Analysis covers the application of the scientific method in the incident response analysis process. An incident responder must consult with CSD leadership if there is any uncertainty on how to properly analyze or handle evidence.

Evaluation criteria may be strictly quantitative, qualitative, or it may include a blended approach to determine prioritization.

Quantitative Criteria

Quantitative criteria focus on *measurable* aspects of an incident, including but not limited to:

- Amount of data affected;
- Type of data affected;
- Number of users affected;
- Number of times the problem has occurred;
- Impact on business operations;
- Financial;
- Customers; and
- Media.

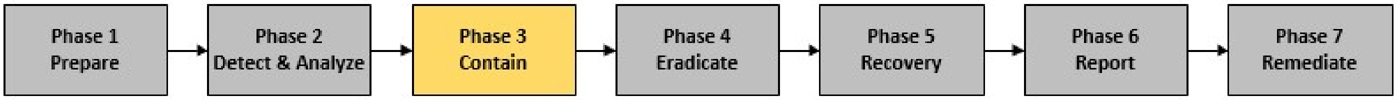
Qualitative Criteria

Qualitative criteria focus on *immeasurable* aspects of an incident, including but not limited to:

- Type of incident;
- Type of system affected;
- Sensitivity/criticality of the data affected;
- Types of users affected;
- Impact on business reputation or legal liability; and
- Public awareness / exposure of incident.

PHASES 3 – CONTAIN

The third phase is "Contain" and these activities focus on containing and controlling the identified cybersecurity incident.



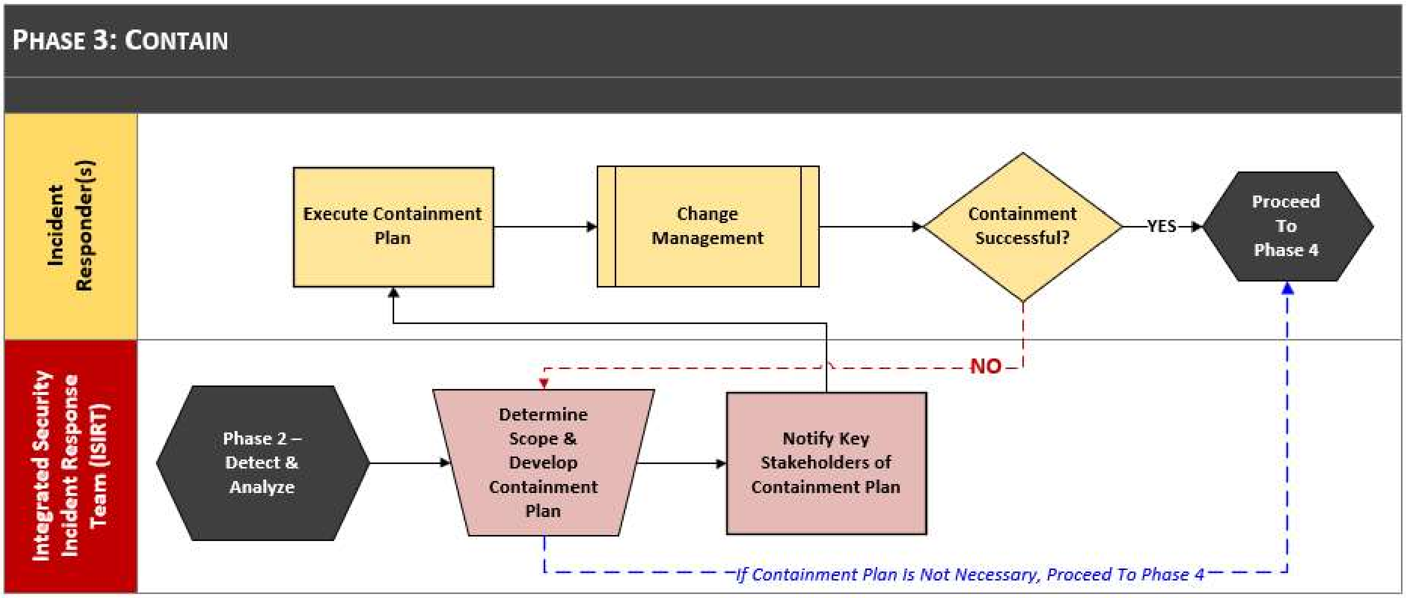
INPUTS

The containment phase includes specific inputs from the identification phase that enable the process to move forward. These inputs include, but are not limited to:

- Incident Details
  - Severity;
  - Classification; and
  - Summary risk assessment.
- Current Incident Status
  - Parties involved;
  - Scope of the incident;
  - Activities currently underway; and
  - Planned activities.
- A list of evidence gathered during the incident investigation

WORKFLOW – CONTAINMENT PROCESS

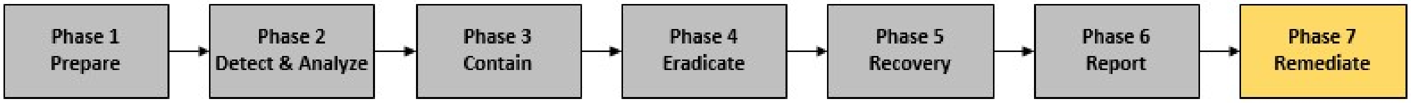
Once an incident is analyzed and prioritized, the incident must be contained.



PHASE 3: CONTAIN
Incident Responder(s)
Integrated Security Incident Response Team (ISIRT)
Execute Containment Plan
Change Management
Containment Successful?
YES
Proceed To Phase 4
NO
Phase 2 – Detect & Analyze
Determine Scope & Develop Containment Plan
Notify Key Stakeholders of Containment Plan
If Containment Plan Is Not Necessary, Proceed To Phase 4

PHASE 7 – REMEDIATE

The last phase is “Remediate” and these activities focus on collecting and consolidating the cybersecurity incident data and transforming it into a Lessons Learned report.



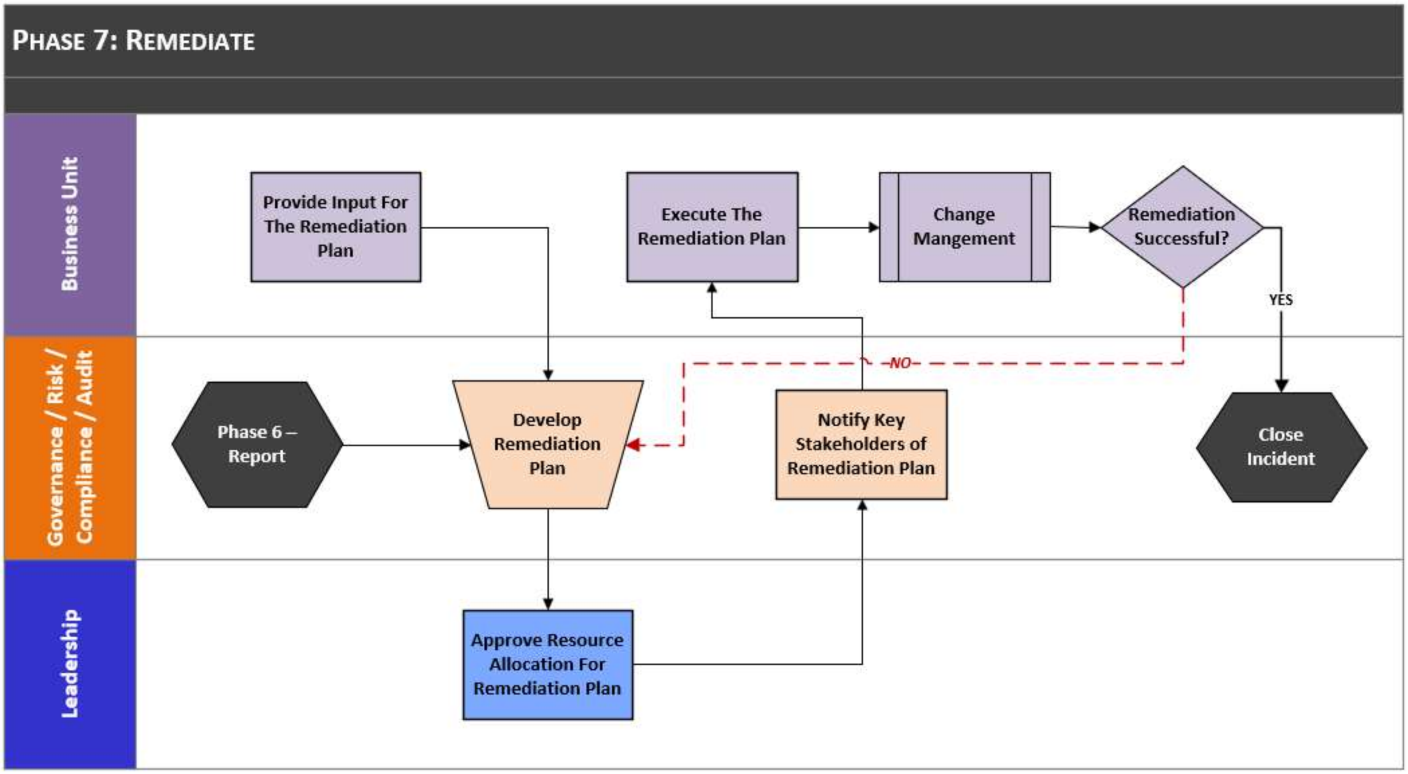
INPUTS

The remediate phase includes specific inputs from the identification phase that enable the process to move forward. These inputs include, but are not limited to:

- After Action Review (AAR) Report;
- Root Cause Analysis (RCA); and
- Risk Register.

WORKFLOW – REMEDIATION PROCESS

Once the recovery of an incident has occurred, remediation needs to take place. The remediation phase focuses on determining the root cause of an incident and how it can be prevented in the future.


PHASE 7: REMEDIATE
Business Unit
Governance / Risk / Compliance / Audit
Leadership
Provide Input For The Remediation Plan
Execute The Remediation Plan
Change Mangement
Remediation Successful?
YES
NO
Phase 6 – Report
Develop Remediation Plan
Notify Key Stakeholders of Remediation Plan
Close Incident
Approve Resource Allocation For Remediation Plan

CYBERSECURITY DEPARTMENT (CSD)

The general concept of CSD operations in this phase include:

- Monitoring for repeat occurrences of the incident.

INFORMATION RISK MANAGEMENT (IRM) / ENTERPRISE RISK MANAGEMENT (ERM)

The general concept of IRM/ERM operations in this phase include:

- Updating the Risk Register, as necessary; and
- Work with BUs on remediation items to ensure risks are adequately resolved.

APPENDIX A: INCIDENT RESPONSE ROLES & RESPONSIBILITIES

This table defines roles and responsibilities for cybersecurity-related incident response:

Role	Description	Responsibilities
Incident Responder	An incident responder is a technical point of contact for acting upon an information security incident. IRs can also be ISIRT team members. There are generally several IRs in any incident who represent different departments.	The incident responder triages the potential incident, determines the nature and scope of the event, and will classify the severity and priority of the incident. The IR is a resource with responsibility to assist in all phases of the information security response lifecycle.
ISIRT Member	An Integrated Security Incident Response Team (ISIRT) Member is the representative contact from a specific functional area or department in case a major information security incident occurs.	An ISIRT Member has the responsibility to assist in the management and resolution of all information security incidents. ISIRT Members temporarily report to the ISIRT Leader for the duration of the incident response operations.
ISIRT Leader	The ISIRT Leader is the appointed leader of the ISIRT for the duration of the incident.	The ISIRT Leader has the ultimate responsibility for the management and resolution of all information security incidents. Serves a single voice of command during an incident. Produces reports and trending analysis to management based on pre-defined KPIs and metrics.
SOC Director	A supervisory role who manages the cybersecurity department Security Operations Center (SOC) and is the first layer of management for cybersecurity incident response.	**ISIRT Support Member.** Responsible for the development and oversight of a comprehensive information security operations program.
Service Desk	Initial Point of Contact (POC) for handling technology-related user escalations.	The service desk is responsible for creating a ticket gathering initial data for potential incidents, and notifying the cybersecurity department SOC.
Information Risk Management (IRM)	Global function that conducts risk assessments and manages risk across the enterprise.	**ISIRT Support Member.** Assists the SOC, ISIRT and business units to develop risk assessments and appropriate remediation steps.
Business Unit (BU)	Distinct department or business function within ACME.	Varies on the BUs capability to resolve technical issues. If the incident is not designated Severity 1 by the cybersecurity department and they have a mature incident resolution process, then they will be responsible resolving the issue. If it is Severity 1, then they will work with risk management to resolve the issue with potential technical triage from a third-party provider.

Appendix C: Scientific Method of Evidence Analysis

The forensic methodology can best be described as more of an art than a science, where the discipline requires flexibility and extensive domain knowledge.

Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. Forensic techniques and expert knowledge are used to explain the current state of a digital artifact. At ACME, the scope of a forensic analysis can vary from simple information retrieval to reconstructing a series of events.

Analysis Process

Evidence-based technical analysis is the process used by CSD to apply the scientific method.

Evidence analysis is a process in which evidence related to an incident is analyzed to learn more about it. While some evidence may provide all the information an examiner might need with a surface examination, often, the evidence needs to be explored more deeply. This process is conducted by an examiner who specializes in the techniques used to analyze evidence, and has been trained in the proper care and handling of evidence, to ensure that evidence is not compromised during the analysis process.

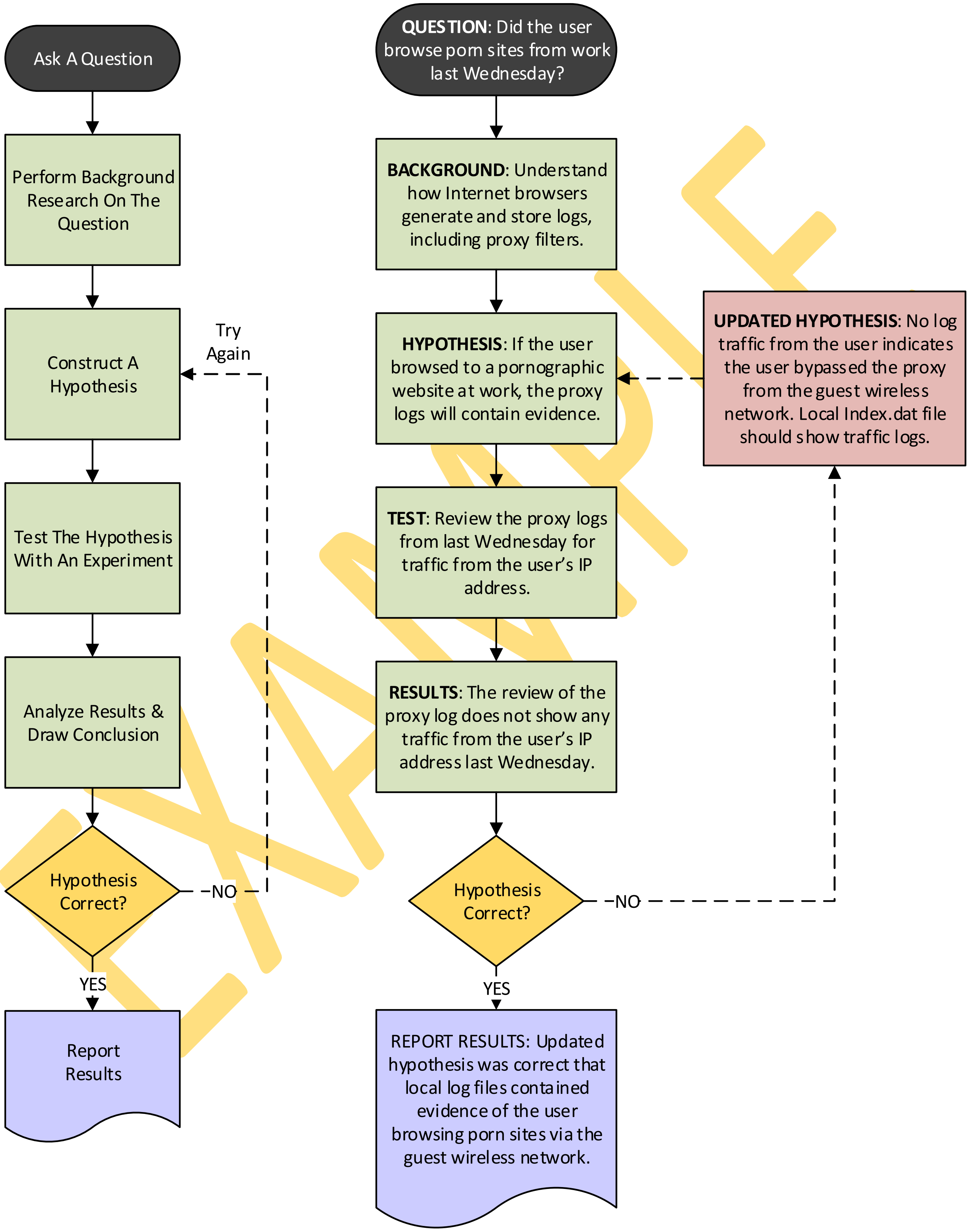
As a reference, Appendix F: Sources of Evidence lists potential evidence sources by type of incident.

Scientific Method

The scientific method is a process for experimentation that is used to explore observations and answer questions. Forensic examiners use the scientific method to search for cause and effect relationships.

Scientific Method – Process Example

The scientific method is a process for experimentation that is used to explore observations and answer questions. Forensic examiners use the scientific method to search for cause and effect relationships.


Ask A Question
Perform Background Research On The Question
Construct A Hypothesis
Test The Hypothesis With An Experiment
Analyze Results & Draw Conclusion
Hypothesis Correct?
NO
Try Again
YES
Report Results
QUESTION: Did the user browse porn sites from work last Wednesday?
BACKGROUND: Understand how Internet browsers generate and store logs, including proxy filters.
HYPOTHESIS: If the user browsed to a pornographic website at work, the proxy logs will contain evidence.
TEST: Review the proxy logs from last Wednesday for traffic from the user's IP address.
RESULTS: The review of the proxy log does not show any traffic from the user's IP address last Wednesday.
Hypothesis Correct?
NO
YES
REPORT RESULTS: Updated hypothesis was correct that local log files contained evidence of the user browsing porn sites via the guest wireless network.
UPDATED HYPOTHESIS: No log traffic from the user indicates the user bypassed the proxy from the guest wireless network. Local Index.dat file should show traffic logs.

Appendix G: Evidence Acquisition

The procedures used by ACME in the acquisition of evidence are adopted from United States Secret Service recommended practices. [23]

There are general principles to follow when responding to any incident scene in which computers and electronic technology may be involved. The most important of those principles are as follows:

- If you reasonably believe that the computer is involved in the crime you are investigating, take immediate steps to preserve the evidence;
- Do not access any computer files. If the computer is off, leave it off;
- If you reasonably believe that the computer is destroying evidence, immediately shut down the computer by pulling the power cord from the back of the computer; and
- If a camera is available, take pictures of the computer (including the screen), the location of the computer and any electronic media attached.

Securing The Evidence

Using the procedures from the Secret Service handbook, there are several common scenarios for data acquisition. These procedures shall be followed, as applicable, and any deviations should be documented by the examiner who secures the evidence:

Desktops & Laptops

Applicability: Desktops and laptops

Procedures: (NOTE - Do not use the computer or attempt to search for evidence)

- Disconnect the network cable.
- Photograph computer front and back as well as cords and connected devices, as found. Photograph surrounding area prior to moving any evidence.
- If computer is “off”, do not turn “on”.
- If computer is “on” and something is displayed on the monitor, photograph the screen.
- If computer is “on” and the screen is blank, move mouse or press space bar (this will display the active image on the screen). After image appears, photograph the screen. If the examiner feels it is necessary to capture volatile memory for the investigation, the examiner will capture an image of volatile memory.
- Powering off the device:
  - DESKTOP: Unplug power cord from back of tower.
  - LAPTOP: If the laptop does not shutdown when the power cord is removed, locate and remove the battery pack. The battery is commonly placed on the bottom, and there is usually a button or switch that allows for the removal of the battery. Once the battery is removed, do not return it to or store it in the laptop. Removing the battery will prevent accidental start-up of the laptop.
- Diagram and label cords to later identify connected devices.
- Disconnect all cords and devices.
- Package components (including any networking gear) and transport / store components as fragile cargo.
- Seize additional storage media, as necessary.
- Keep all media, including tower, away from magnets, radio transmitters and other potentially damaging elements.
- Collect instruction manuals, documentation and notes, as necessary.
- Document all steps involved in the seizure of a computer and components.

[23] United States Secret Service. “Best Practices For Seizing Electronic Evidence (v3): A Pocket Guide for First Responders.”