Incident Response Training

North Central Texas Council of Governments

Incident Response Training

Part 5 –

Table Top Exercise

IR Material to use

www.stealth-iss.com

ADMINISTRATION

- IR Framework
- IR Standard
- IR Organizations

IR Plan

- Incident Categorization
- IR Organization Structure
- IR Roles and Responsibilities
- IR Response Times / SLAs
- IR Tracking and Reporting

TECHNICAL REQUIREMENTS

- Incident Response Tool Kit

INCIDENT RESPONSE

- IR Notification Form
- IR Management Log
- IR SOPs
- Forensics Intake Form
- Chain of Custody
- IR Report Template
- IR Financial Tracker
- Regulatory Notification Requirements
- IR Customer and Media Communication
- IR Lessons Learned Form

SOPs for Key Incidents:

DDoS Attack
Ransomware/Malware
Data Theft
Elevation of Privileges
Improper Computer Usage
Phishing
Root Access
Virus Outbreak

IR Where to start

Microsoft Word Document

IR Document Usage List

Microsoft Word Document

IR Acronyms

Microsoft Word Document

Tabletop Exercise – What?

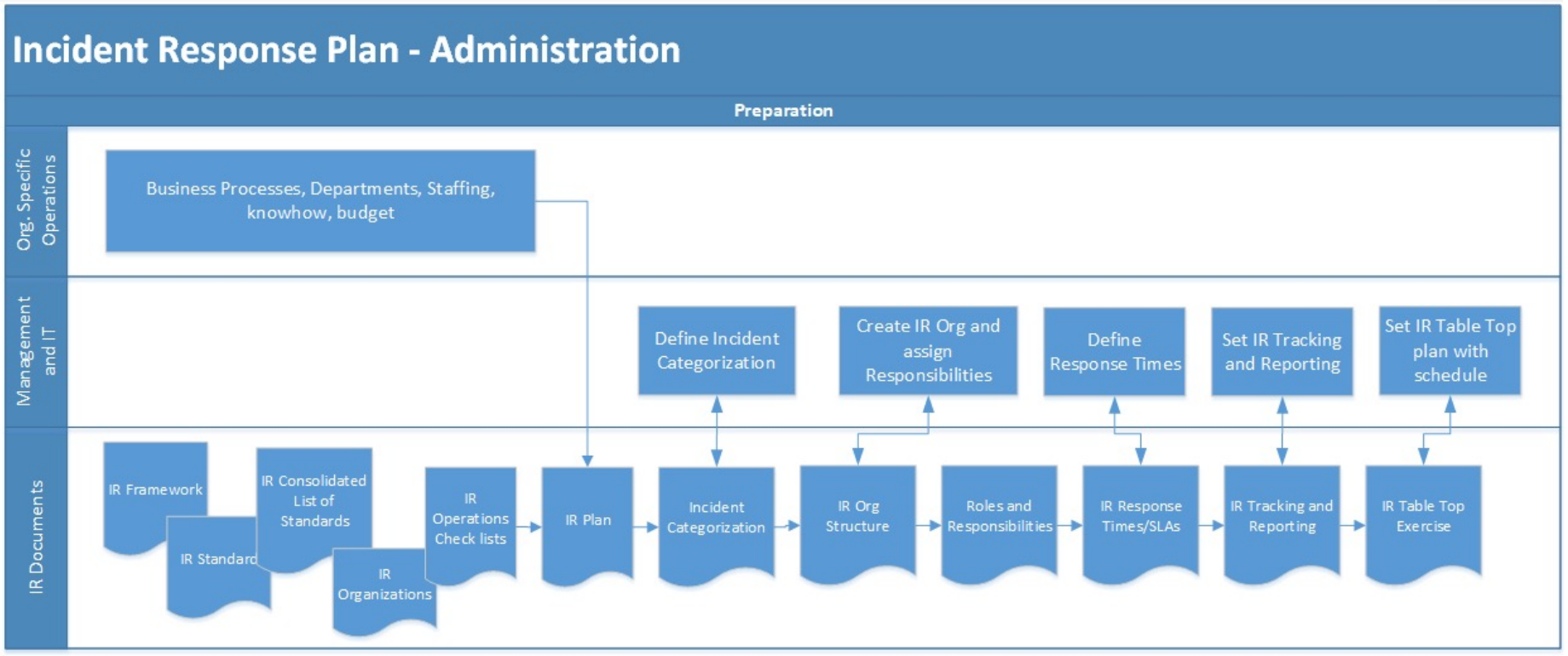
- Effective way to evaluate your incident response plans through practice using example incidents/scenarios
- Choose (most relevant) and address various scenarios
- Test validate processes to be used following and emergency event
- IR Team familiarity and advance collaboration - Incident Commander (IC), Cybersecurity Incident Response Team (CIRT), Incident Handling Team (IHT), Human Resources function, and Business Continuity Members

Tabletop Exercise – Why?

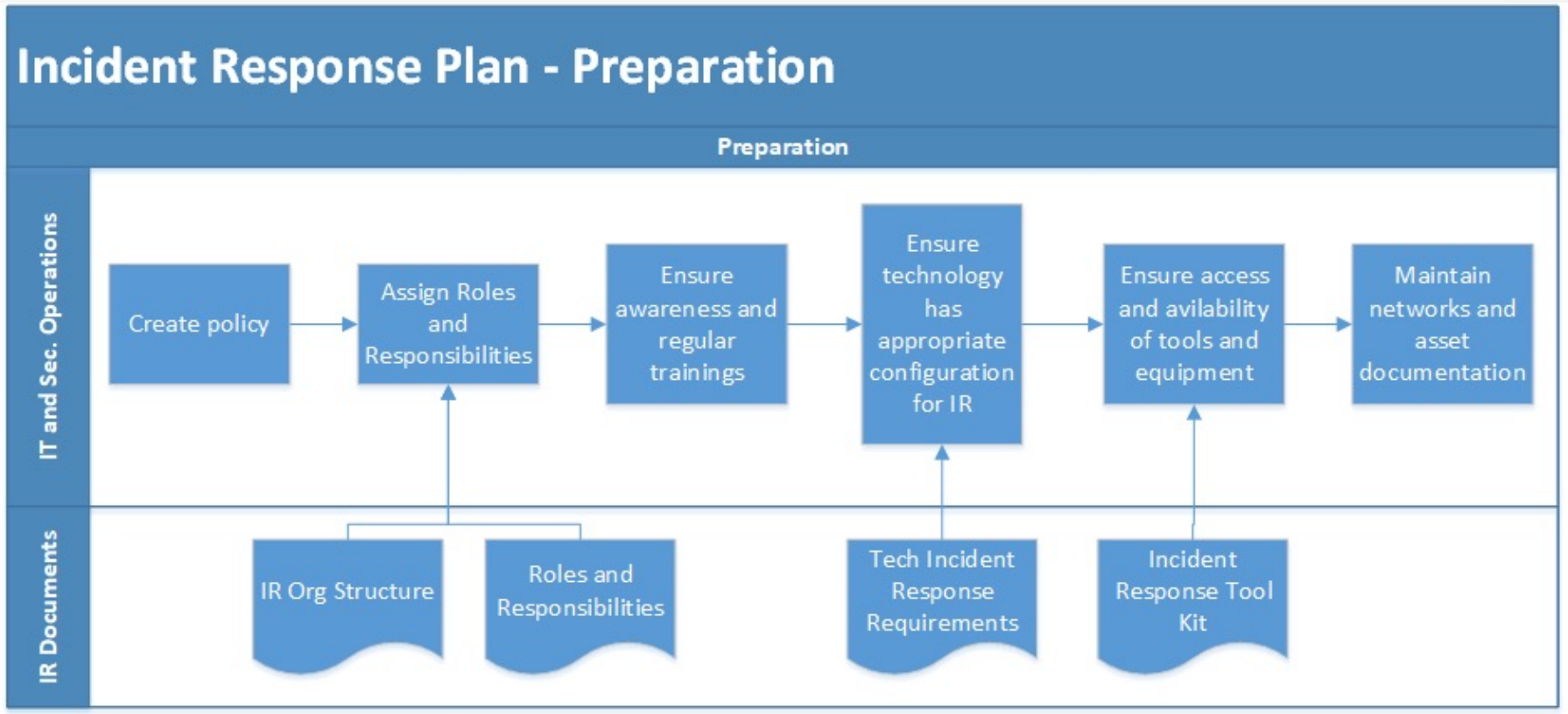
Reduce time to restore business operations in the event of a breach

- Help your people understand their roles and responsibilities
- Develop a better understanding of breaches and how to deal with, even prevent them
- Cost-effective way of ramping up your security defenses
- Assess and promote communication and collaboration within teams and departments, identify gaps
- List out the strengths and weaknesses of the IR processes, improve the processes
- Identify any training gaps
- Potentially Identify loopholes or defects in the Plan
- Regulatory requirement: mandatory for critical national infrastructure and banking

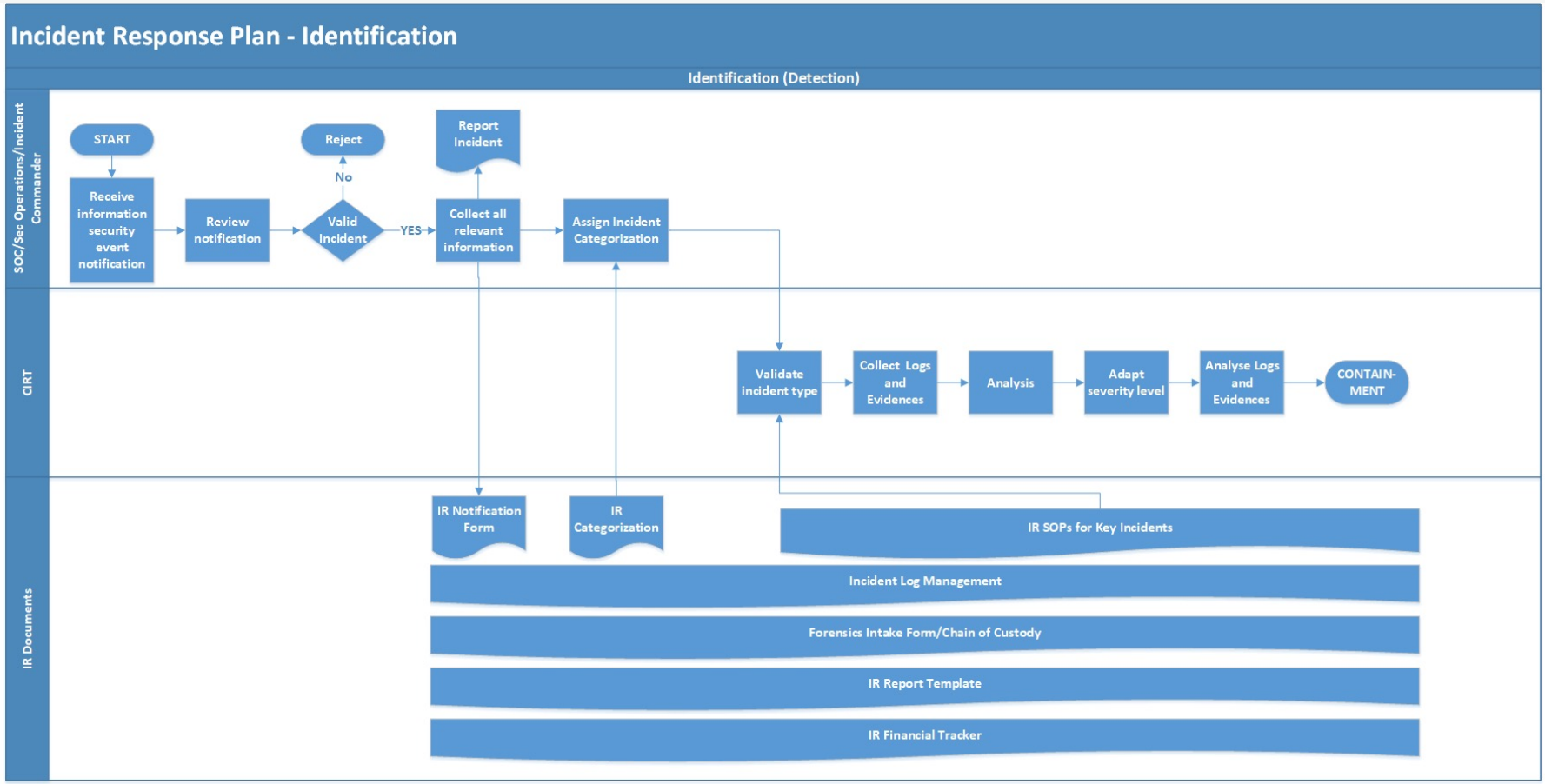
IR Process



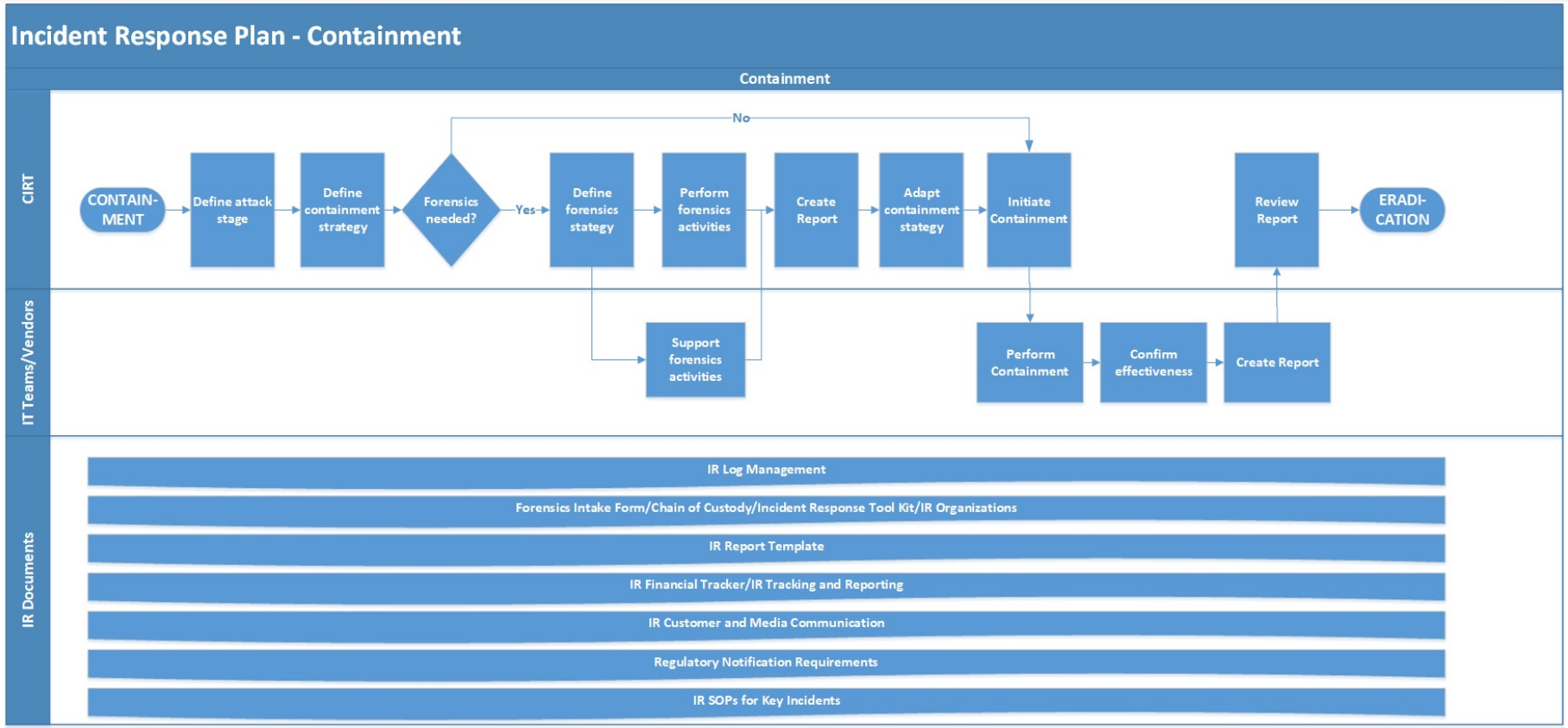
IR Process



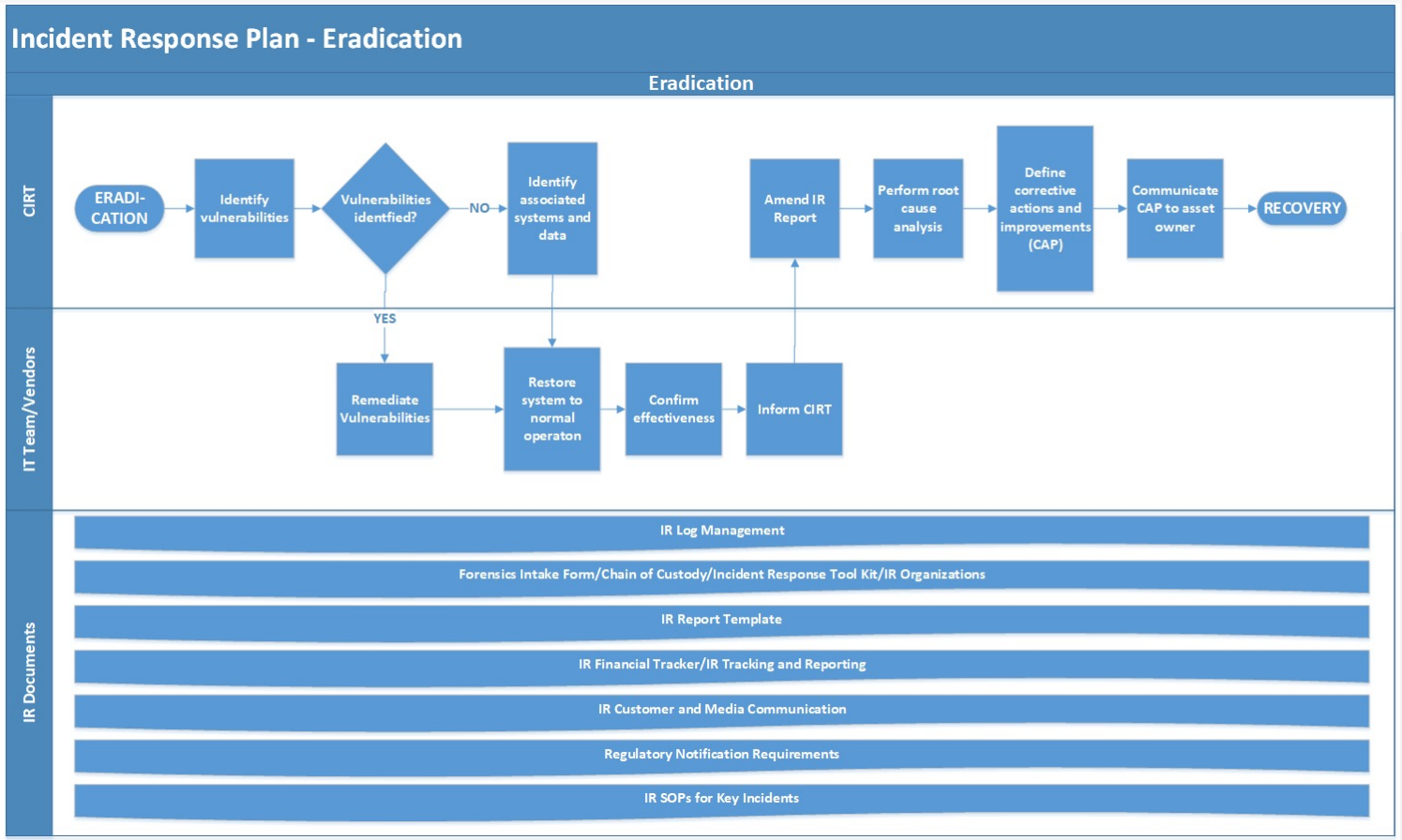
IR Process



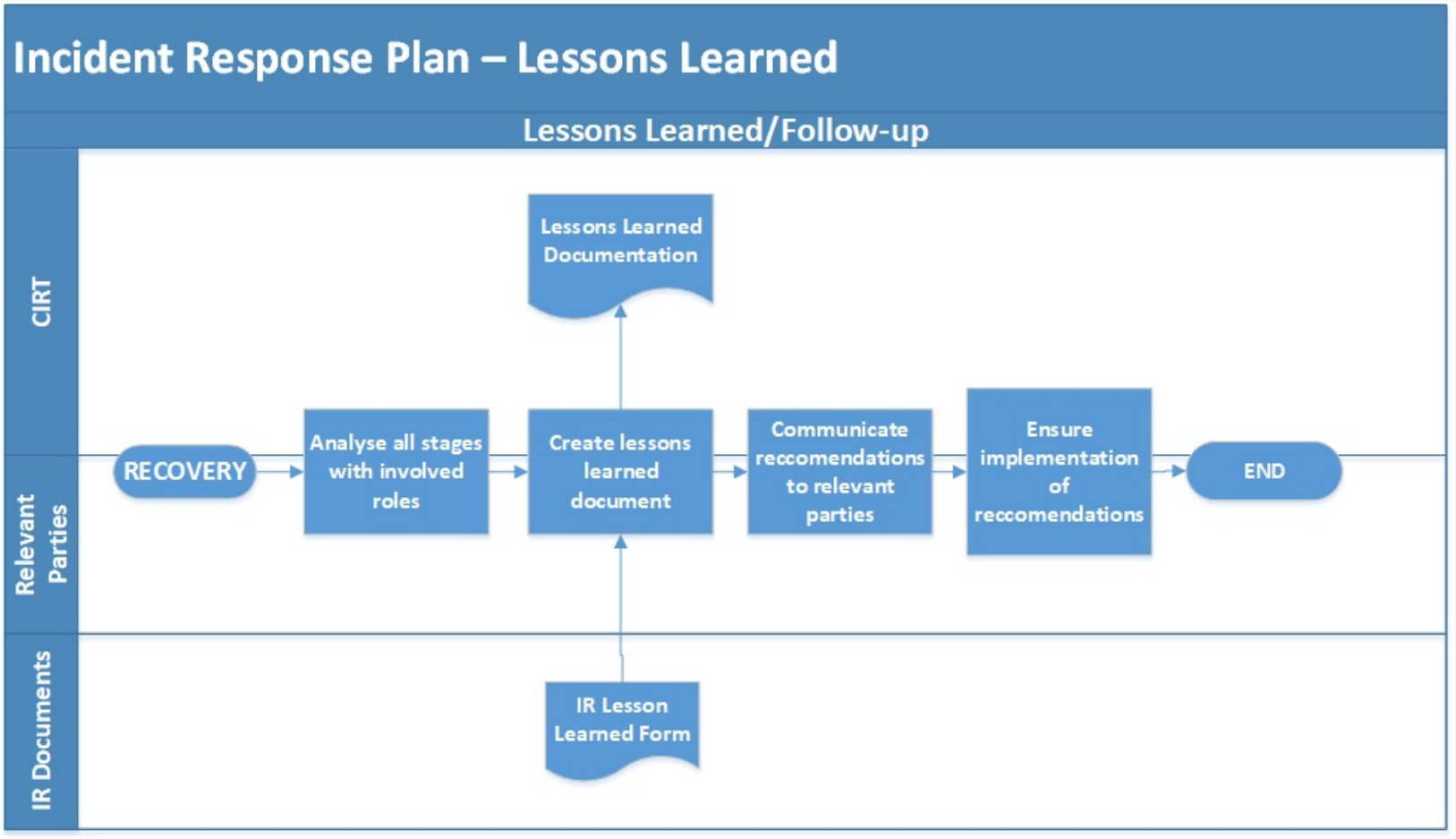
IR Process



IR Process



IR Process



Scenario: Cloud Storage Compromise

Scenario:

One of your organization's internal departments frequently uses outside cloud storage to store large amounts of data, some of which may be considered sensitive.

You have recently learned that the cloud storage provider that is being used has been publicly compromised and large amounts of data have been exposed. All user passwords and data in the cloud provider's infrastructure may have been compromised.

Scenario: Ransomware Attack on Commission

Scenario: Orchestrated by an unknown assailant, a ransomware DDOS attack takes place against XYZ Public Utility Commission. There is concern that the attack will spread to utilities if the assailant uses private contact information stored with the commission's network to launch a phishing campaign. However, there is no evidence to suggest that this is the attacker's intent.

Update: It is seemingly a typical day at the commission, and operations are running smoothly. However, the PUC's IT department notices a series of abnormal spikes in activity within one of their systems. The peaks are initially dismissed as routine fluctuations, and the day continues as usual.

Update: A few hours later, the commission's website crashes due to a high volume of traffic. The PUC's IT department realizes that the commission is currently under a Distributed Denial of Service (DDOS) attack, explaining the abnormal fluctuations from earlier.

Update: Three hours after the initial discovery of the DDOS attack, a commission staffer receives an email claiming to be a hacker. The hacker states that they will continue to execute daily DDOS attacks on the commission unless the PUC pays them. To make matters worse, the hacker claims to have access to Personally Identifiable Information (PII) from employees and customers and demand payment. If you do not pay, the hacker threatens to release the PII publicly. The hacker copies members of the press on the email.

Scenario: CYBER ATTACK

Foreign Actors, wanting a ransom of 1 million dollars have determined that shutting down Organization's systems. They do their research and determine all supporting providers involved that support the organizations system. Ransomware has been propagated from one of the affected ISPs and the organization has possibly been affected by Ransomware on one of their servers and the 2 data centers hosting their infrastructure.

Assumptions:

- All systemic components of the organizations systems including Hardware systems and application servers, communication routers, disk data storage sub-systems, Operating Systems, and backup systems are supported at the "Location 1" and "Location 2" data centers.
- Calls have been successfully routed to the organization.
- All components of the organizations systems are configured in a High Availability (HA) failover configuration.
- All data backups are stored and current between the 2 data centers.
- Recovery may be needed to recover the organizations systems at the current site or fail over to the secondary site.
- All organizations personnel are available at this time
-

Key Issues:

- At this time, we only know of one organization being affected by ransomware.
- We do not know if other/similar organizations are also a target.
- We still do not have all the details, as information we have is not complete and slow to come in.

The Scenario: CYBER ATTACK – Decision Making

- What is the immediate response and what are planning considerations at this time for the organization?
  - What are the priorities?
  - Is this an incident to activate the Incident Commander and deploy the Incident Handling Team?

- List what preparation steps should be taken.

- What information is required to make an informed decision?

- What communications need to be sent? And who will provide those communication?
  - Communications between the organization and regional centers?
  - Communications internally?
  - Communication with other organization support vendors?
  - Communications external to the media?
  - Communications to other customers?
  - Communications between organization and regional ISPs?

- When is it appropriate to invoke the Incident Response Plan?

The Scenario: CYBER ATTACK – Resources & Comms

Resources

- What resources are readily available for this event?
  - List resources that will be needed
- What resources are required if data needs to be recovered?
- What resources may be needed from other areas within the region? (i.e., third parties, ISPs, regional emergency/incident offices?)
- What resources, if any, are needed from external sources?
- What response workstreams within existing teams will need to be setup for the response?

Communication

- What is the key message/s, at this time and who would be sending to the internal team, public, vendors, customers, business partners and government officials at this time?

Questions?

Where to find documents and information?

https://nctcog.org/ep/resources/cyber-security-incident-response-planning-system

THANK YOU

HQ – ARLINGTON, VIRGINIA

4601 North Fairfax Drive, Suite 1200
Arlington, VA 22203

OFFICE LOCATIONS

Las Vegas, Nevada

London, England

Dubai, United Arab Emirates

Bratislava, Slovakia

www.stealth-iss.com