

Incident Response Training

North Central Texas Council of Governments
Incident Response Training

**Part 2 –
The Incident Response Plan (“the Plan”)**



Agenda



1. Incident Response Plan
2. IR Plan Key Components
 - Incident Categorization
 - Response Times, Notification and Communication
 - IR Contact List
3. Incident Response
 - Identification
 - Containment
 - Eradication
 - Lessons Learned



Agenda



1. **Incident Response Plan**
2. IR Plan Key Components
 - Incident Categorization
 - Response Times, Notification and Communication
 - IR Contact List
3. Incident Response
 - Identification
 - Containment
 - Eradication
 - Lessons Learned



The Incident Response Plan



An incident response plan:

- Is the most important document in Incident Response
- Defines the mission
- Outlines procedures, steps, and responsibilities
- Defines the approach to incident response and activities required in each phase of incident response
- Assigns roles and responsibilities for completing
- Maintains a contact and escalation list (internal and external)

May include several documents:

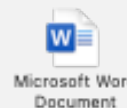
- Organization, Roles and Responsibilities
- IR Table-Top Exercises
- **Incident Categorization**
- **IR Reponses Times and SLAs**
- **Contact lists**

Agenda



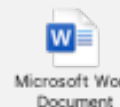
1. Incident Response Plan
2. IR Plan Key Components
 - **Incident Categorization**
 - Response Times, Notification and Communication
 - IR Contact List
3. Incident Response
 - Identification
 - Containment
 - Eradication
 - Lessons Learned





Key Components: Incident Categorization – P1

Description	Priority Level	Category
<p>A security incident will be assigned as “Priority Level 1/High” is the incident is characterized by the following:</p> <ul style="list-style-type: none">– The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. <p>AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.</p>	P1	HIGH



Key Components: Incident Categorization – P2

Description	Priority Level	Category
<p>A security incident will be assigned as “Priority Level 2/Moderate” if the incident is characterized by the following:</p> <ul style="list-style-type: none">– The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. <p>AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:</p> <ul style="list-style-type: none">(i) cause a significant degradation in mission capability to an extent and duration that the organization is unable to perform its primary functions, but the effectiveness of the functions is significantly reduced;(ii) result in significant damage to organizational assets;(iii) result in significant financial loss; or(iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.	P2	MODERATE



Key Components: Incident Categorization – P3

Description	Priority Level	Category
<p>A security incident will be assigned as “Priority Level 3/Low” if the incident is characterized by the following:</p> <ul style="list-style-type: none">– The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.² <p>AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:</p> <ul style="list-style-type: none">(i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;(ii) result in minor damage to organizational assets;(iii) result in minor financial loss; or(iv) result in minor harm to individuals.	P3	LOW

Agenda



1. Incident Response Plan
2. IR Key Components
 - Incident Categorization
 - **Response Times, Notification and Communication**
 - IR Contact List
3. Incident Response
 - Identification
 - Containment
 - Eradication
 - Lessons Learned



Key Components: Response Times and SLAs

At a minimum, the following should occur within this initial response time:

- Initial assessment and triage.
- Case classification is determined.
- The case ownership is established/Incident Commander (IC) is assigned.
- Confirmation email will be sent to the IC/reporter/organization/department. This is the initial “we have your case” email.

Criticality Level	Initial Response Time	Ongoing Response (Critical Phase)	Ongoing Response (Resolution Phase)	Ongoing Communication Requirement
1	60 Minutes	Cybersecurity Incident Response Team (CIRT) Incident Commander assigned to work case on 24x7 basis.	Incident Commander assigned to work on case during normal business hours.	Case update sent to appropriate parties on a daily basis during critical phase. If CIRT involvement is necessary to restore critical systems to service then case update will be sent a minimum of every 2 hours. Case update sent to appropriate parties on a weekly basis during resolution phase.
2	4 Hours	CIRT Incident Commander assigned to work case on 24x7 basis.	CIRT Incident Commander assigned to work on case during normal business hours.	Case update sent to appropriate parties on a daily basis during critical phase. Case update sent to appropriate parties on a weekly basis during resolution phase.
3	48 Hours	Case is worked as CIRT time/resources are available.	Case is worked as CIRT time/resources are available.	Case update sent to appropriate parties on a weekly basis.
4	72 Hours	Case is worked as CIRT time/resources are available.	Case is worked as CIRT time/resources are available.	Case update sent to appropriate parties on a weekly basis.

Key Components: Notification and Communication

Key areas:

- Internal communication and escalations
- External Communication
 - Public Media
 - Customers
 - Providers
- Regulatory Compliance

Tooling:

- Incident tracking
- Chat room
- Video chat
- Documentation tool
- Status page
- Secure File Share

Personnel	VP	Senior Leaders	Response Mgmt.	Extended Support BALs, Legal, Partners	Directors	Depts.	Media	Clients	Enterprise
Incident Commander	P / B		A / B, V, E	P / B, V, E	P / V, E				
CIRT			P / B, V, E	A / B, V, E	A / V, E	A / B, V, E			
Communication							P / B, V, E	P / B, V, E	
IT Management/C TO/CEO/CISO		P / B, V, E				P / B, V, E			P / B, V, E

Responsibility	Type	
P = Primary Responsibility	B = Briefing	Communication frequency shall be established based on the nature of the incident and SLAs.
A = Alternate Responsibility	E = Email	
	V = Voice Mail	

Agenda



1. Incident Response Plan
2. IR Key Components
 - Incident Categorization
 - Response Times, Notification and Communication
 - **IR Contact List**
3. Incident Response
 - Identification
 - Containment
 - Eradication
 - Lessons Learned



Key Components: Contact Lists

Successful Incident Resolutions rely on effective communication and escalation:

- Full and current contact list with primary and secondary contacts (email, phone, names)
 - Understand when to contact and when to escalate
 - External partner contacts are key
-
- Contact list to be regularly updated and tested
 - On call schedule may be needed

www.stealth-iss.com

External Contacts			Main	Additional								
Organization	Address		###-###-####	###-###-####								
FBI	Technical Assessment Team											
Secret Service	First & Last	Primary	name@Organization.com	###-###-#### x##	###-###-#### ####	###-###-#### x##						
Physical Security	First & Last	Secondary	name@Organization.com	###-###-####	###-###-####	###-###-####						
NIMS	<table border="1"> <thead> <tr> <th>Name</th> <th>Role</th> <th>E-mail</th> <th>Work</th> <th>Mobile</th> <th>Alternate</th> </tr> </thead> </table>						Name	Role	E-mail	Work	Mobile	Alternate
Name	Role	E-mail	Work	Mobile	Alternate							
CERT	Extended Team											
FEMA	First & Last	Legal	First & Last	Primary	name@Organization.com	###-###-#### x##	###-###-#### ####	###-###-#### x##				
	First & Last	Insurance	First & Last	Secondary	name@Organization.com	###-###-#### x##	###-###-#### ####	###-###-#### x##				
	First & Last	Primary	First & Last	Tertiary	name@Organization.com	###-###-#### x##	###-###-#### ####	###-###-#### x##				
	First & Last	Secondary	Cybersecurity Incident Response Team (CIRT)									
	First & Last	Primary	name@Organization.com	###-###-#### x##	###-###-#### ####	###-###-#### x##						
	First & Last	Secondary	name@Organization.com	###-###-#### x##	###-###-#### ####	###-###-#### x##						

Agenda

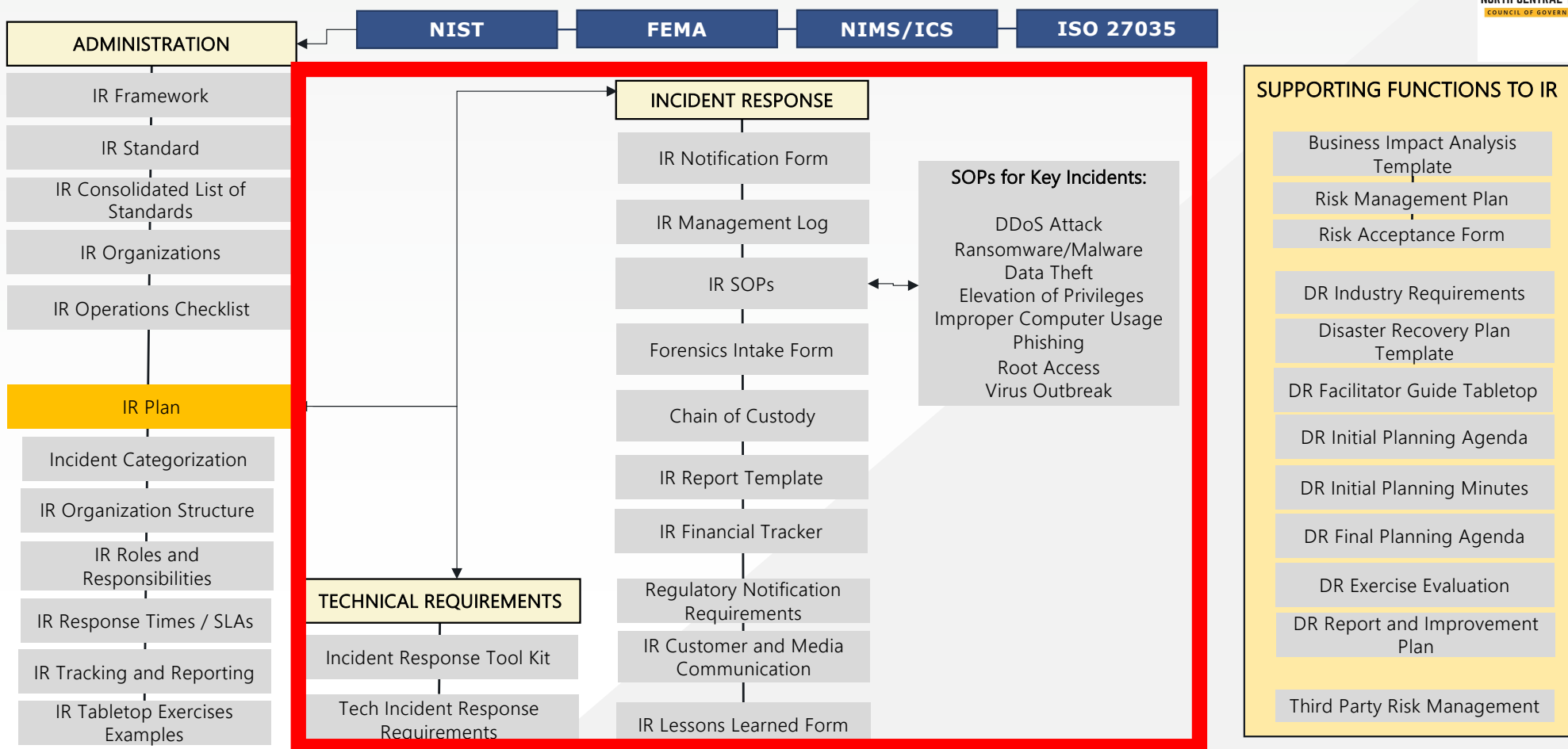


1. Incident Response Plan
2. IR Key Components
 - Incident Categorization
 - Response Times, Notification and Communication
 - IR Contact List
3. **Incident Response**
 - **Identification**
 - **Containment**
 - **Eradication**
 - **Lessons Learned**



IR Aligned with Standards

www.stealth-iss.com

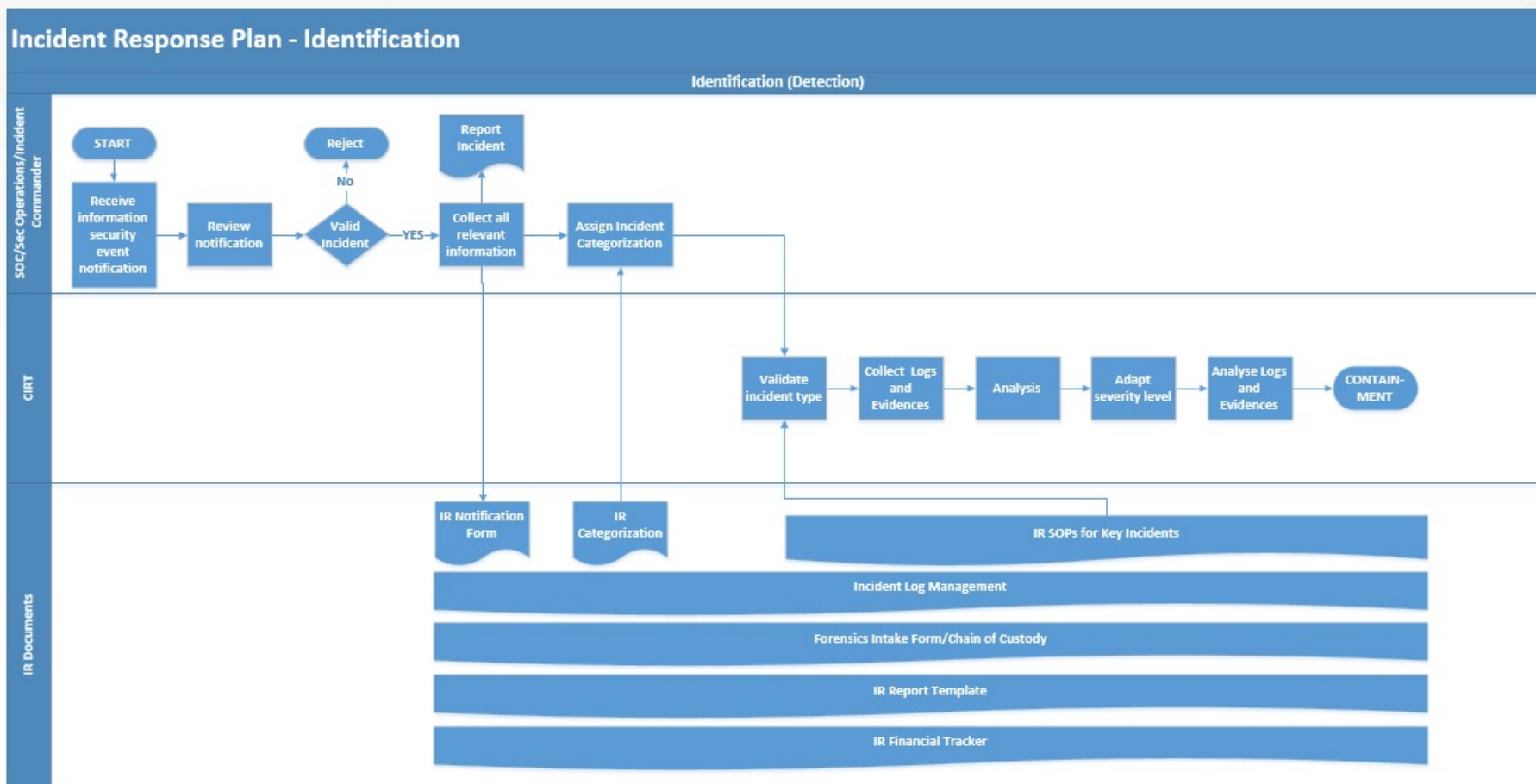


Incident Response Process – What now



Incident Response Process – Identification

www.stealth-iss.com

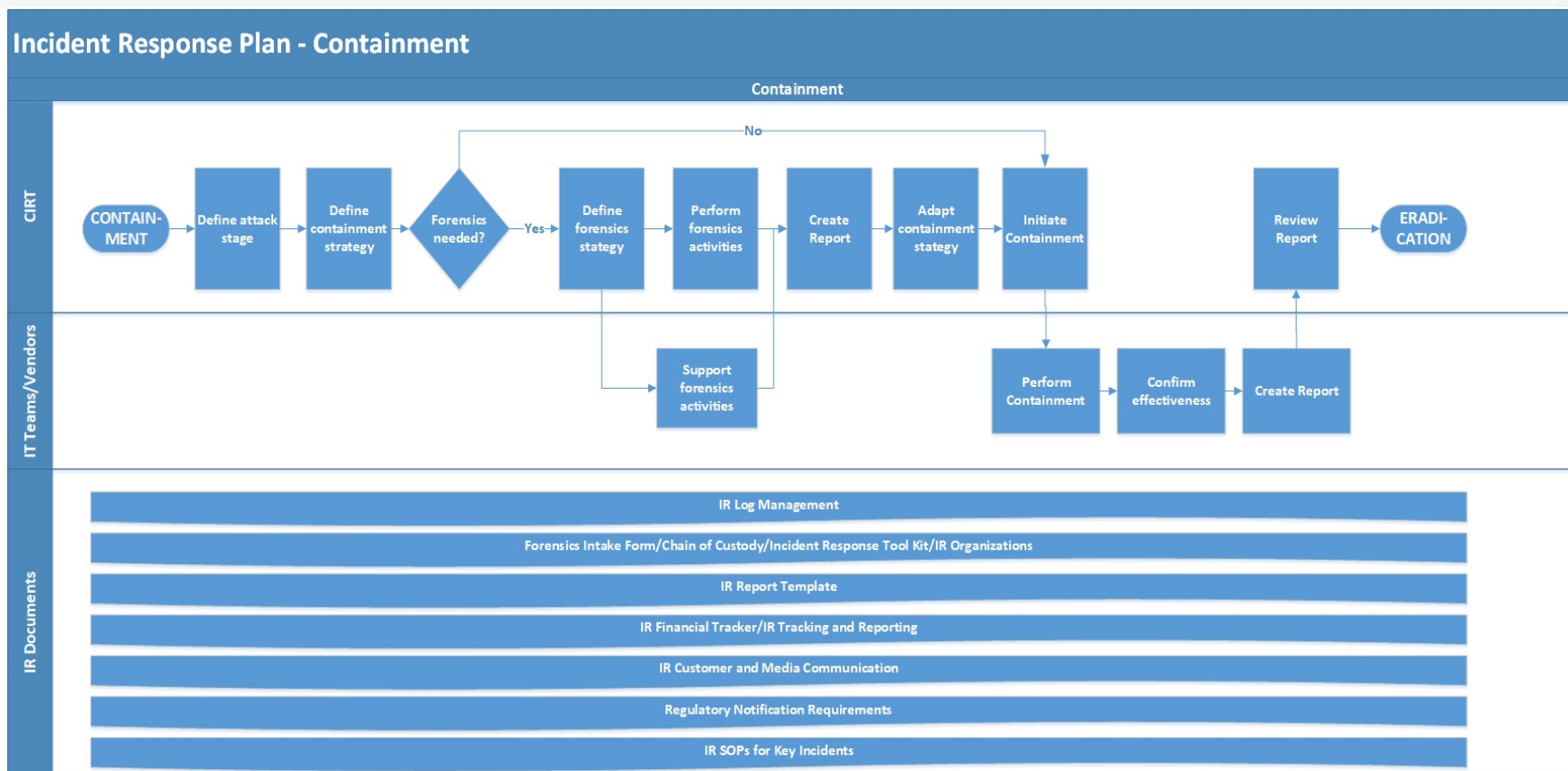


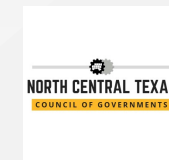
Incident Response Process – Identification

www.stealth-iss.com

Documents to use	To Be used	
IR Notification Form	Always	  Microsoft Word Document Microsoft Word Document
IR Categorization	Always	 Microsoft Word Document
Incident Log Management	Always	 Microsoft Word Document
IR SOPs for Key Incidents	Always	 Microsoft Word Document
Forensics Intake Forms	Large/Critical	 Microsoft Word Document
Chain of Custody	Large/Critical	 Microsoft Word Document
IR Report Template	Medium/Large	 Microsoft Word Document
IR Financial Tracker/Tracker	Medium/Large	 Microsoft Word Document











Incident Response Process – Containment



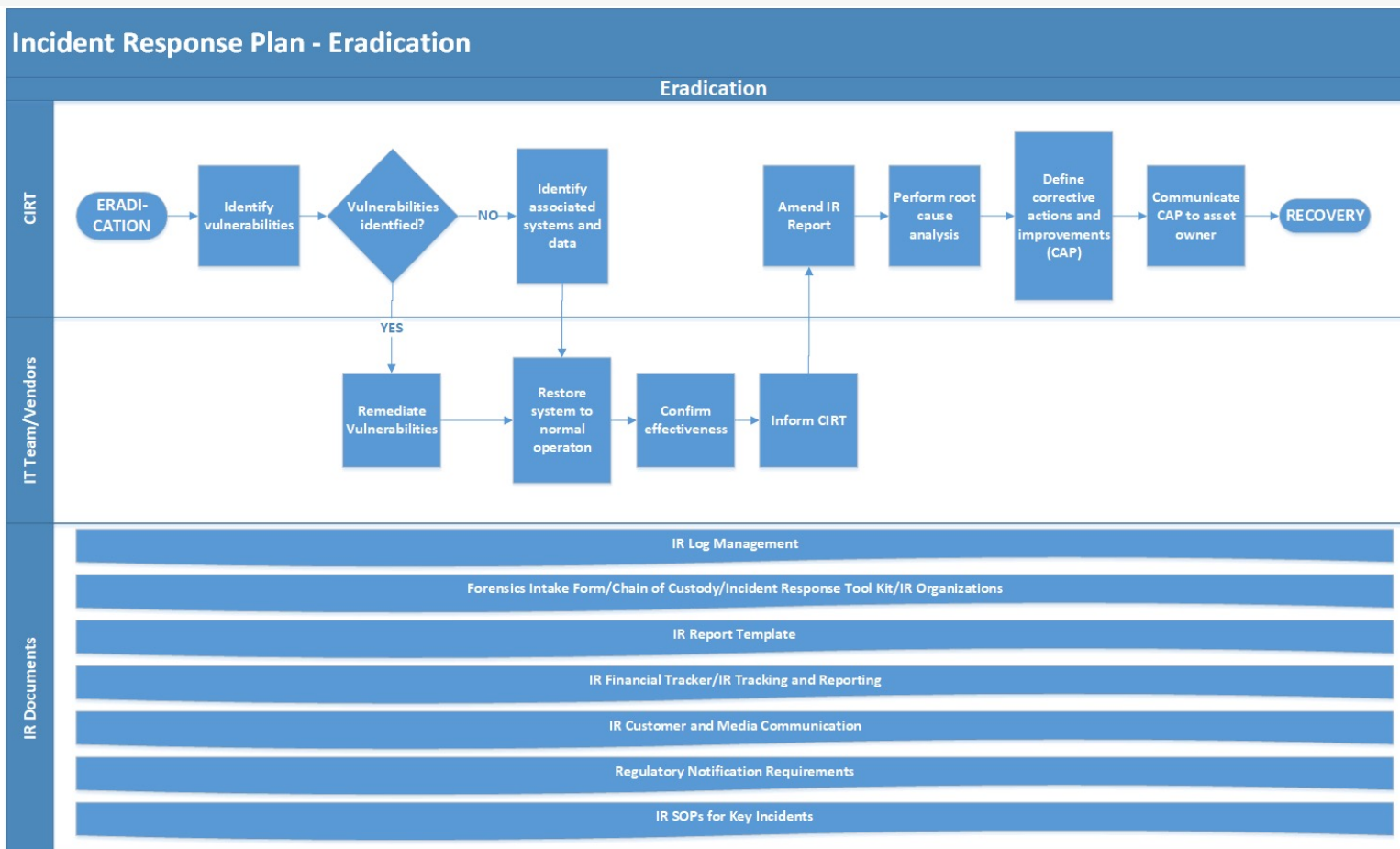


Incident Response Process – Containment

www.stealth-iss.com

Documents to use	To Be used	
Incident Response Toolkit	Always	 Microsoft Word Document
IR Organizations	Always	 Microsoft Word Document
Incident Log Management	Always	 Microsoft Word Document
IR SOPs for Key Incidents	Always	 Microsoft Word Document
Forensics Intake Form/Chain of Custody	Large/Critical	 Microsoft Word Document
IR Report Template	Medium/Large	 Microsoft Word Document
IR Financial Tracker/IR Tracking	Medium/Large	 Microsoft Word Document
IR Customer and Media Notification	Medium/Large	 Microsoft Word Document
Regulatory Notification Requirements	Medium/Large	 Microsoft Word Document
		 Microsoft Word Document











Incident Response Process – Eradication



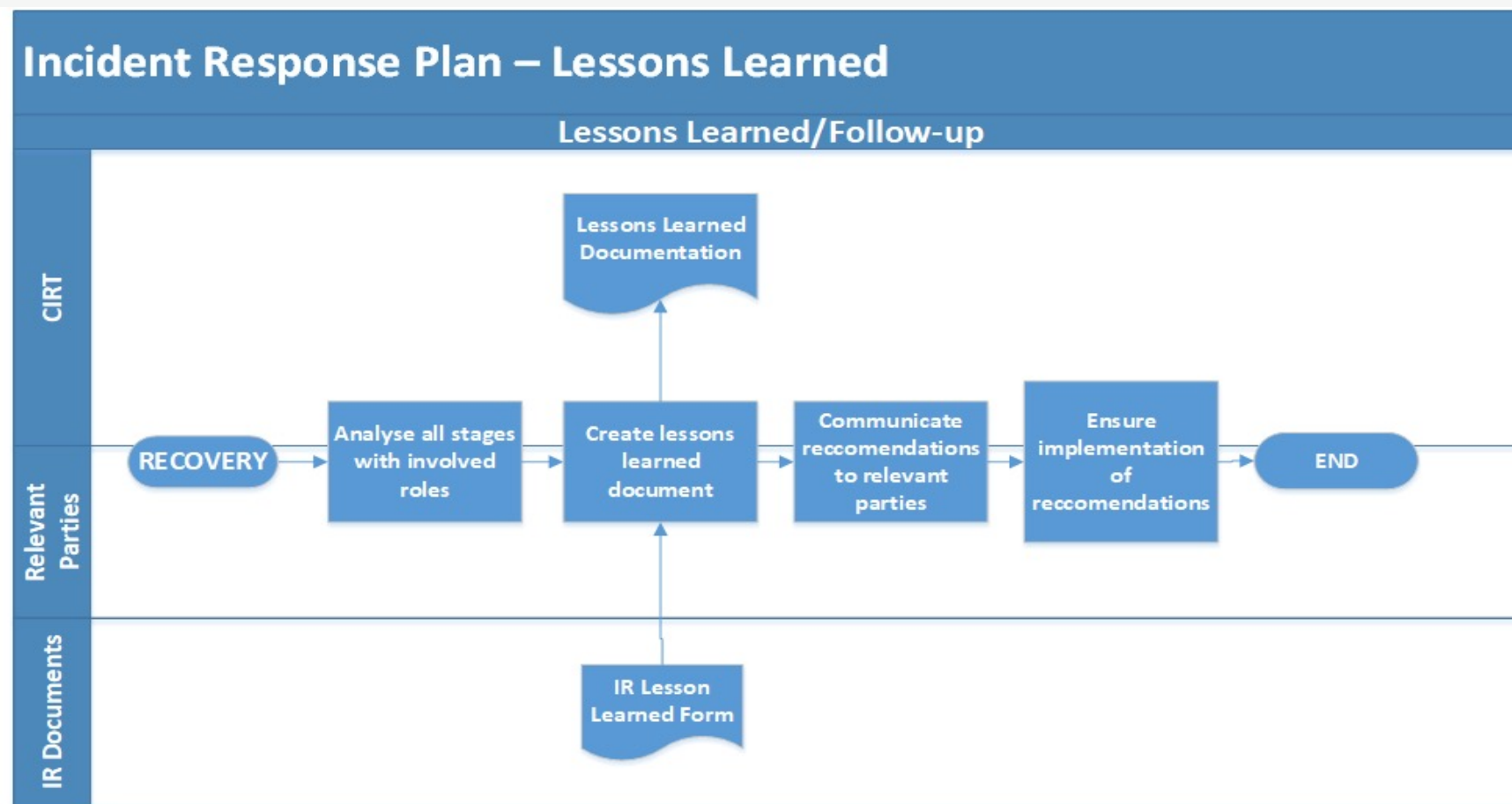


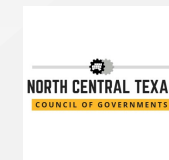
Incident Response Process – Eradication

www.stealth-iss.com


Documents to use	To Be used	
Incident Response Toolkit	Always	 Microsoft Word Document
IR Organizations	Always	 Microsoft Word Document
Incident Log Management	Always	 Microsoft Word Document
IR SOPs for Key Incidents	Always	 Microsoft Word Document
Forensics Intake Form/Chain of Custody	Large/Critical	  Microsoft Word Document Microsoft Word Document
IR Report Template	Medium/Large	 Microsoft Word Document
IR Financial Tracker/IR Tracking	Medium/Large	 Microsoft Word Document
IR Customer and Media Notification	Medium/Large	 Microsoft Word Document
Regulatory Notification Requirements	Medium/Large	 Microsoft Word Document

Incident Response Process – Lessons Learned



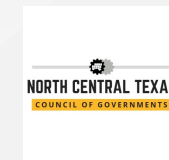


Incident Response Process – Lessons Learned

Documents to use	To Be used	
IR Lessons Learned	Always	 Microsoft Word Document

Questions?





Where to find documents and information?

www.stealth-iss.com

The screenshot shows the website for the North Central Texas Council of Governments. The header includes the organization's name, a navigation menu with categories like Agency Administration, Aging Services, Economic Development, Emergency Preparedness, Environment & Development, Executive Director, NCT 9-1-1, Public Safety, Regional Data, Workforce Solutions, and Transportation. There are also search and language options. The main content area features a breadcrumb trail: Home > Emergency Preparedness > Resources > Cyber Security Incident Response Planning System. The title of the page is "Cyber Security Incident Response Planning System". Below the title, the workshop date is listed as December 14, 2021. The workshop schedule is as follows:

- 9:00 - 9:20 - Introduction
- 9:20 - 10:15 - Incident Response - The Big Picture
- 10:30 - 11:30 - "The Plan", in detail
- 11:45 - 12:45 - Communication & Reporting
- Lunch Break
- 1:30 - 2:30 - Risk Management & Disaster Recovery
- 2:45 - 4:00 - Tabletop Exercise

To the right of the text is an image of a computer screen displaying a "System HACKED" warning with a yellow triangle and exclamation mark icon, set against a background of blue code and data visualizations.

<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



Stealth-ISS Group® Inc. | www.stealth-iss.com | bizdev@stealth-iss.com