Incident Response Training

North Central Texas Council of Governments

Incident Response Training

Training Overview

Structure

1. The Goal
2. How is this training set up?
3. What is Incident Response?
4. Why this project and training?
5. Who will benefit from this?
6. Where and How to use the IR Material
7. Questions

Structure

1. **The Goal**
2. How is this training set up?
3. What is Incident Response?
4. Why this project and training?
5. Who will benefit from this?
6. Where to find and how to use the IR Material
7. Questions

The Goal

Provide Cybersecurity Incident Response resources to:

- Prepare for a potential Cybersecurity Incident
- Know what to do and how to do it
- Know the location of correct documents, templates and tools
- Know who to contact to request local/regional/state/federal or third-party help
- Facilitate Incident Resolution
- Communicate with regional/state teams using established standards
- Align all Incident Management activities with NIMS (National Incident Management System)

Result:

- A centralized and comprehensive repository within NCTCOG SharePoint including:
  - Comprehensive collection of Incident Response documentation for plans and standards
  - Incident Response processes
  - Forms and report guidelines
  - Contact and communication lists
  - Recorded Training Videos

The Right People, Plan, Tools

Structure

1. The Goal
2. **How is this training set up?**
3. What is Incident Response?
4. Why this project and training?
5. Who will benefit from this?
6. Where and How to use the IR Material
7. Questions

How is this training set up?

- Incident Response – the big picture
  - Overview of IR and NIMS
  - Organizations
- “The Plan” – in detail
  - How to prepare
  - Documents and Forms to use
  - Incident Response Process
- Communication and Reporting
  - Regulatory requirements
  - Clients and Customers
  - Reporting and KPIs
- Risk Management and Disaster Recovery
  - Third Parties
  - Business Impact Analysis
- Incident Response Tabletop Exercise

Structure

1. The Goal
2. How is this training set up?
3. **What is Incident Response?**
4. Why this project and training?
5. Who will benefit from this?
6. How to use the IR Material
7. Where to find documents and information?
8. Questions

What is Incident Response?

Incident response is an **organized approach** to addressing and managing a potential breach or aftermath of a security breach.

The goal is to handle the situation in a way that **limits damage** and **reduces recovery time and costs.**

The Right People, Plan, Tools

What is Incident Response?

Components of Incident Response?

- The Incident Response Plan (“the Plan”)
- A list of roles and responsibilities
- A list of types of incidents requiring action
- The current state of the network infrastructure and security safeguards
- Detection, investigation and containment procedures
- Steps toward eradication
- Steps toward recovery
- The breach notification process
- A list of follow-up tasks
- A call list
- Incident response plan testing
- Any revisions/lessons learned

Structure

1. The Goal
2. How is this training set up?
3. What is Incident Response?
4. **Why this project and training?**
5. Who will benefit from this?
6. Where and How to use the IR Material
7. Questions

Why this project and training?

Structure

1. The Goal
2. How is this training set up?
3. What is Incident Response?
4. Why this project and training?
5. **Who will benefit from this?**
6. Where and How to use the IR Material
7. Questions

Who will benefit from this knowledge?

Federal, State, Local, Education, Commercial entities which:

- Use or subscribe to IT services (in-house or in-cloud)
- Are at risk of cyber security incidents (malware, ransomware, accidents etc.)
- Collaborate with other entities to deliver services
- May have a significant operational or financial impact if their services cannot be delivered
- May cause significant hardship to others if their services cannot be delivered

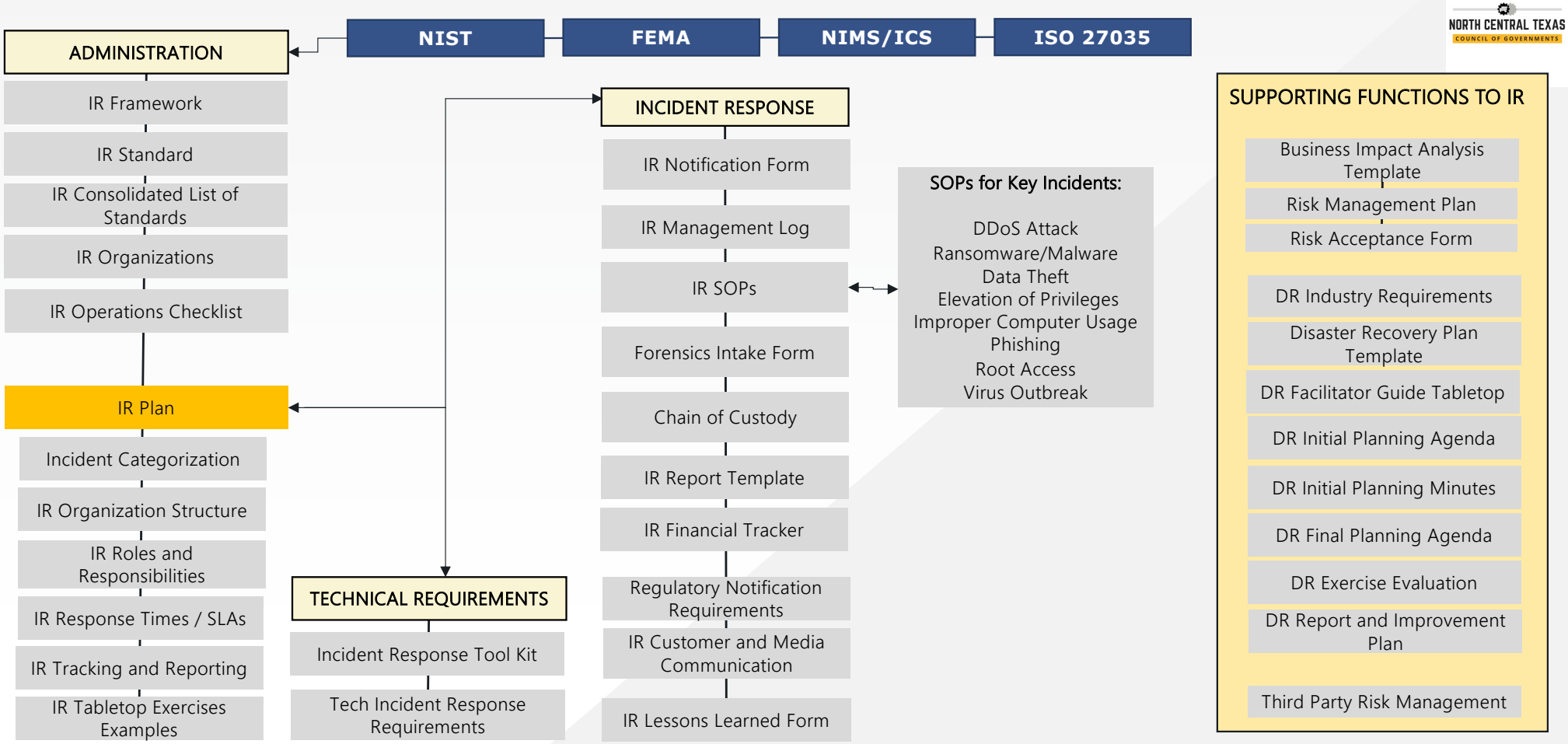
Organizational Staff:

- The Organizational Manager
- All Executives including Chief Information/Technology or Security Officer
- Incident Commander (“IC”)
- IT and IT Security Staff including CIRT resources
- Human Resources
- Finance Teams
- Health and Safety
- Data Privacy and Risk Officers
- Any staff member involved with incident or emergency management at local/regional/state and federal level

Structure

1. The Goal
2. How is this training set up?
3. What is Incident Response?
4. Why this project and training?
5. Who will benefit from this?
6. **Where and How to use the IR Material**
7. Questions

How to use the IR Material



Where to find documents and information?

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

Questions?

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