

Incident Response Training

North Central Texas Council of Governments
Incident Response Training

**Part 4 –
Risk Management and Disaster Recovery**



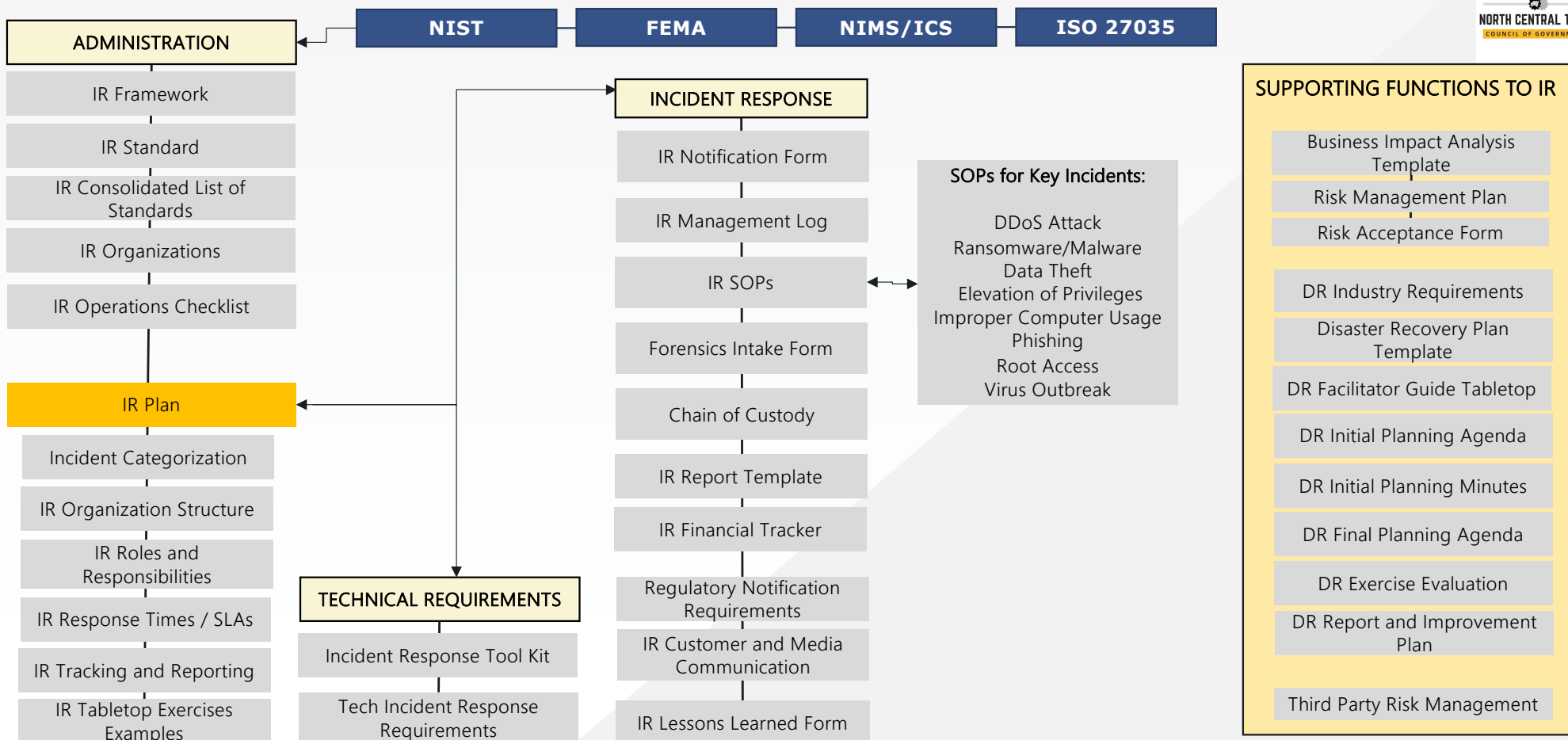
Agenda



1. IR Risk Management and Disaster Recovery
2. Risk Analysis, Management and Risk Register
3. Business Impact Analysis
4. Third Party Risk
5. Disaster Recovery Plan and Management



How to use the IR Material



Agenda



1. **IR Risk Management and Disaster Recovery**
2. Risk Analysis, Management and Risk Register
3. Business Impact Analysis
4. Third Party Risk
5. Disaster Recovery Plan and Management



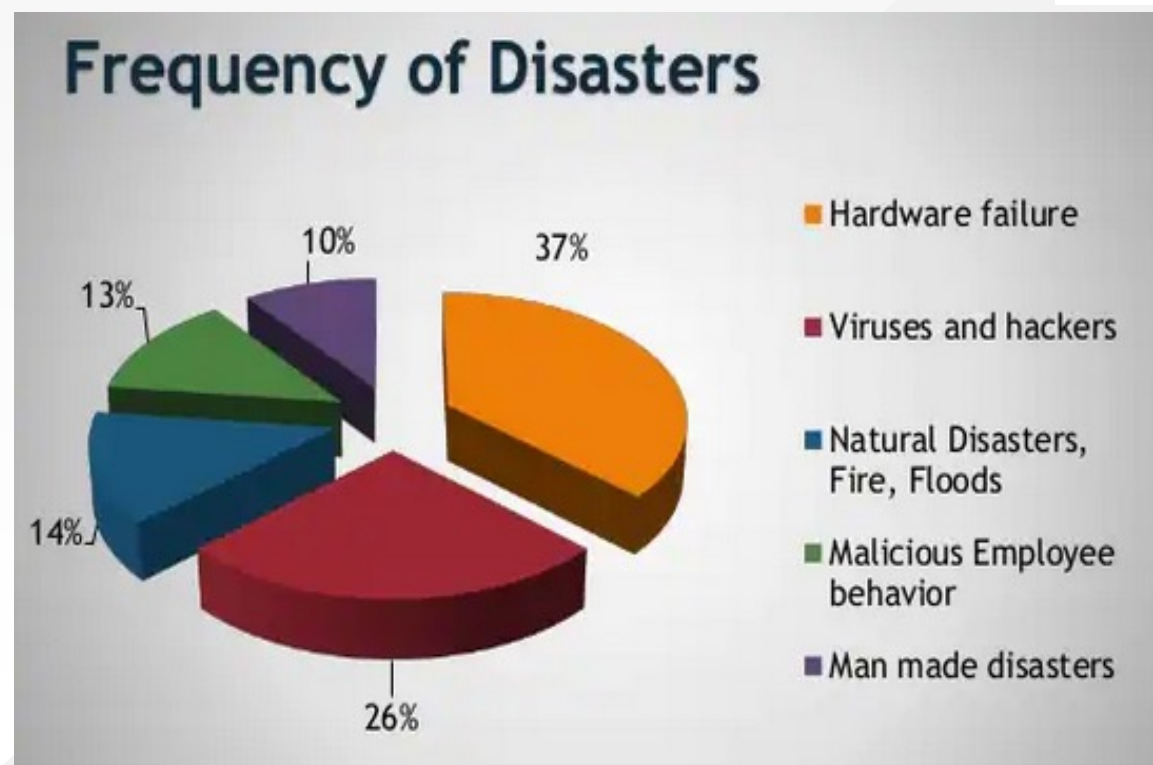
Risk Management and Disaster Recovery

Disaster Recovery:

The strategic and detailed planning for the timely restoration of information technology, network and data following a disaster

Risk Management:

The forecasting and evaluation of risks together with the identification of procedures to avoid or minimize their impact.



Agenda

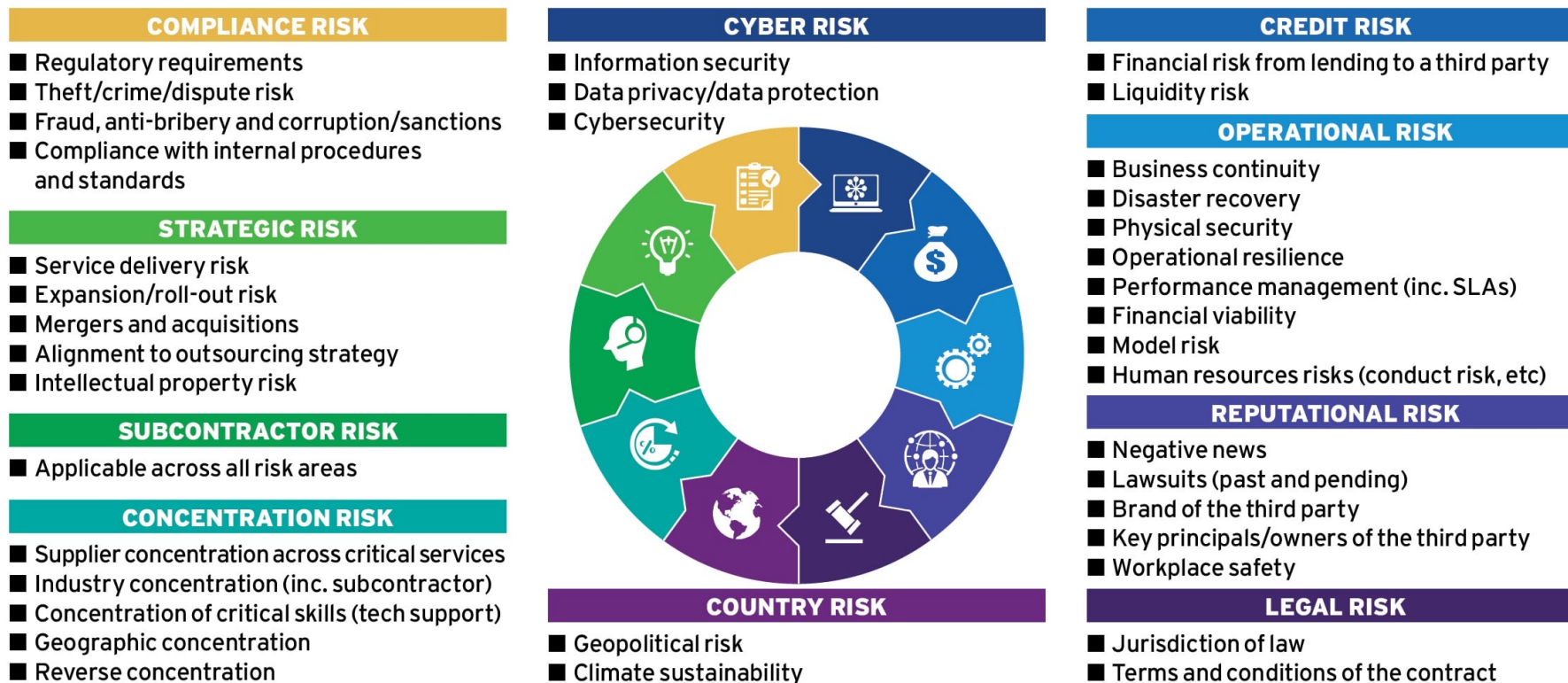


1. IR Risk Management and Disaster Recovery
2. **Risk Analysis, Management and Risk Register**
3. Business Impact Analysis
4. Third Party Risk
5. Disaster Recovery Plan and Management



Risk Analysis, Management and Risk Register

FIGURE 2: RISK ASSESSMENT PROCESS - WHAT ARE THE POTENTIAL AREAS OF THIRD PARTY RISK?



2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Co-operative (KPMG International), a Swiss entity. All rights reserved.

Agenda



1. IR Risk Management and Disaster Recovery
2. Risk Analysis, Management and Risk Register
3. **Business Impact Analysis**
4. Third Party Risk
5. Disaster Recovery Plan and Management



Business Impact Analysis

- What disasters could occur?
- Which business processes are of strategic importance?
- What IT assets support those business processes (internal and external)?
- What impact would they have on the organization financially? Legally? On human life? On reputation?
- What is the required recovery time period?

Identifies assets required for business to recover and continue doing business

BIA may be based on multiple worst-case scenarios

BIA should contain security breach scenarios

Key assets include critical resources, systems, facilities, personnel, and records

Identifies recovery times

Used for information security and non-information security purposes

Identifies adverse effects on the organization

Identifies key components

Agenda



1. IR Risk Management and Disaster Recovery
2. Risk Analysis, Management and Risk Register
3. Business Impact Analysis
4. **Third Party Risk**
5. Disaster Recovery Plan and Management



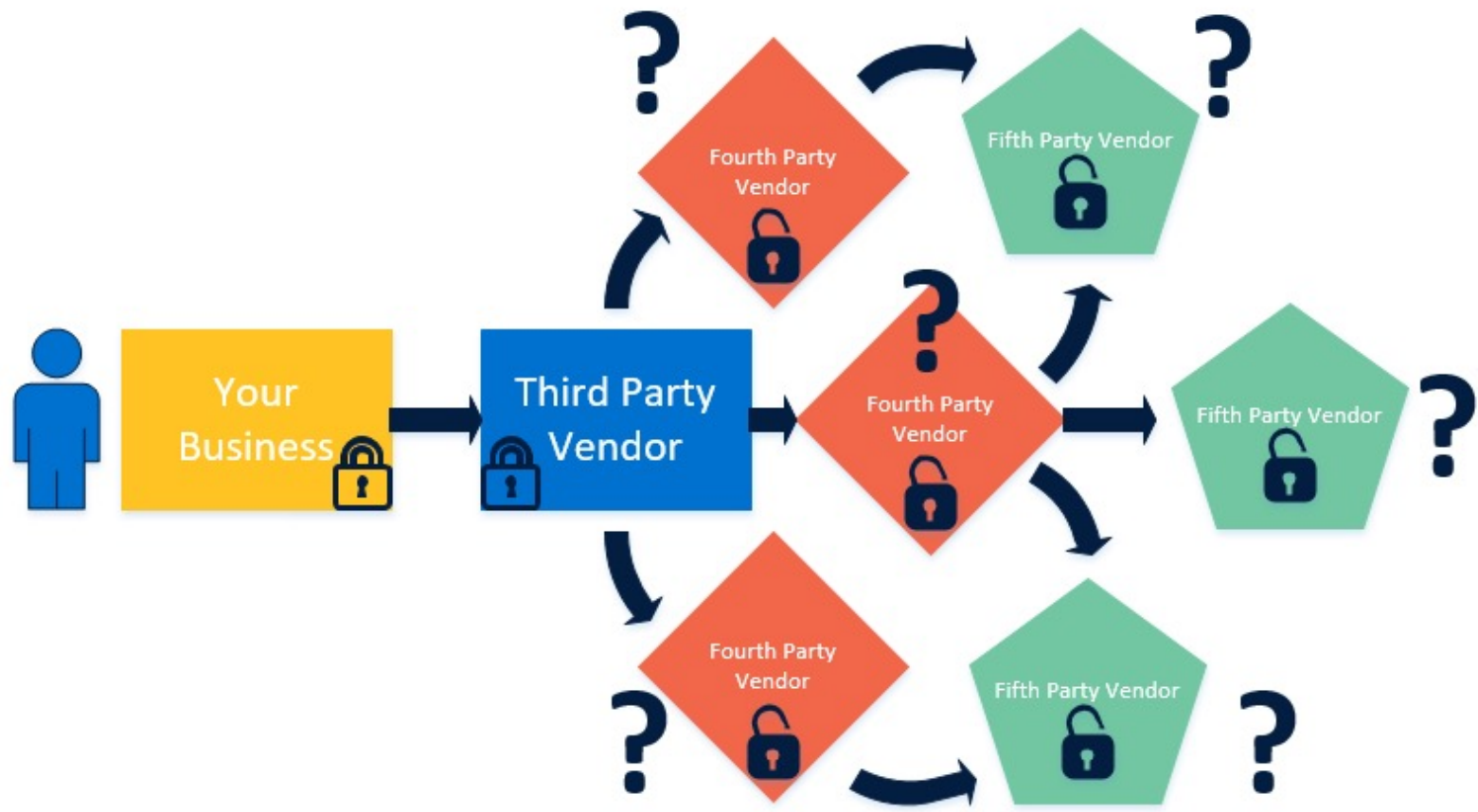
Third Party Risk

Third Parties:

- Outsourced Cleaning Crew
- IT Vendor/Managed Service Provider
- Printer Management Company
- Software Providers
- Cloud Services
- Data Processing Companies
- Outsourced HR



Fourth Party Risk



Agenda



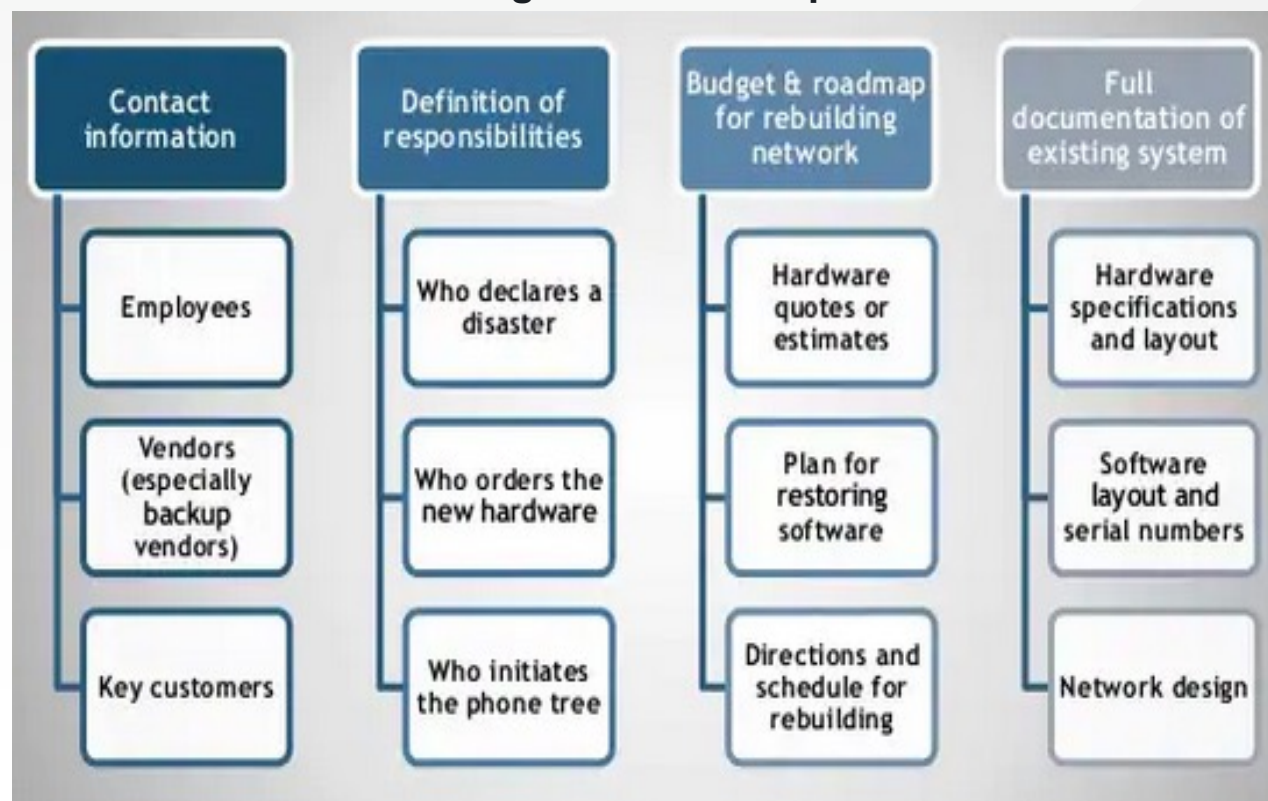
1. IR Risk Management and Disaster Recovery
2. Risk Analysis, Management and Risk Register
3. Business Impact Analysis
4. Third Party Risk
5. **Disaster Recovery Plan and Management**












Disaster Recovery Plan

- Written document with policies, step-by-step procedures and responsibilities
- Must be tested (or exercised) frequently
- DR is a regulatory requirement for many industries

What goes into a DR plan



Disaster Recovery Management

Documents to use	
DR Requirements Industries	  Microsoft Word Document Microsoft Word Document
IT Disaster Recovery Plan Template	 Microsoft Word Document
DR Facilitator Guide Tabletop Exercise	    Microsoft Word Document Microsoft Word Document Microsoft Word Document Microsoft Word Document
DR Planning Agendas and Minutes (Initial and Final)	
DR Exercise Evaluation	 Microsoft Word Document
DR Report and Improvement Plan	 Microsoft Word Document

Questions?





Where to find documents and information?

The screenshot shows the website for the North Central Texas Council of Governments. The header includes the organization's name, navigation menus for various services (Agency Administration, Aging Services, Economic Development, Emergency Preparedness, Environment & Development, Executive Director, NCT 9-1-1, Public Safety, Regional Data, Workforce Solutions, Transportation), and a search bar. 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

The image shows a computer screen with a blue background. A yellow warning triangle with an exclamation mark is prominently displayed in the center. Below the triangle, the text "System HACKED" is written in white. The background of the screen shows blurred code and data, suggesting a cybersecurity context.

<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



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