CISA ELECTION SECURITY SERVICES BRIEFING

Ernesto Ballesteros, JD, MS, CISSP, CISA, Security+
State Cybersecurity Coordinator of Texas
Region 6 | Texas

About CISA

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

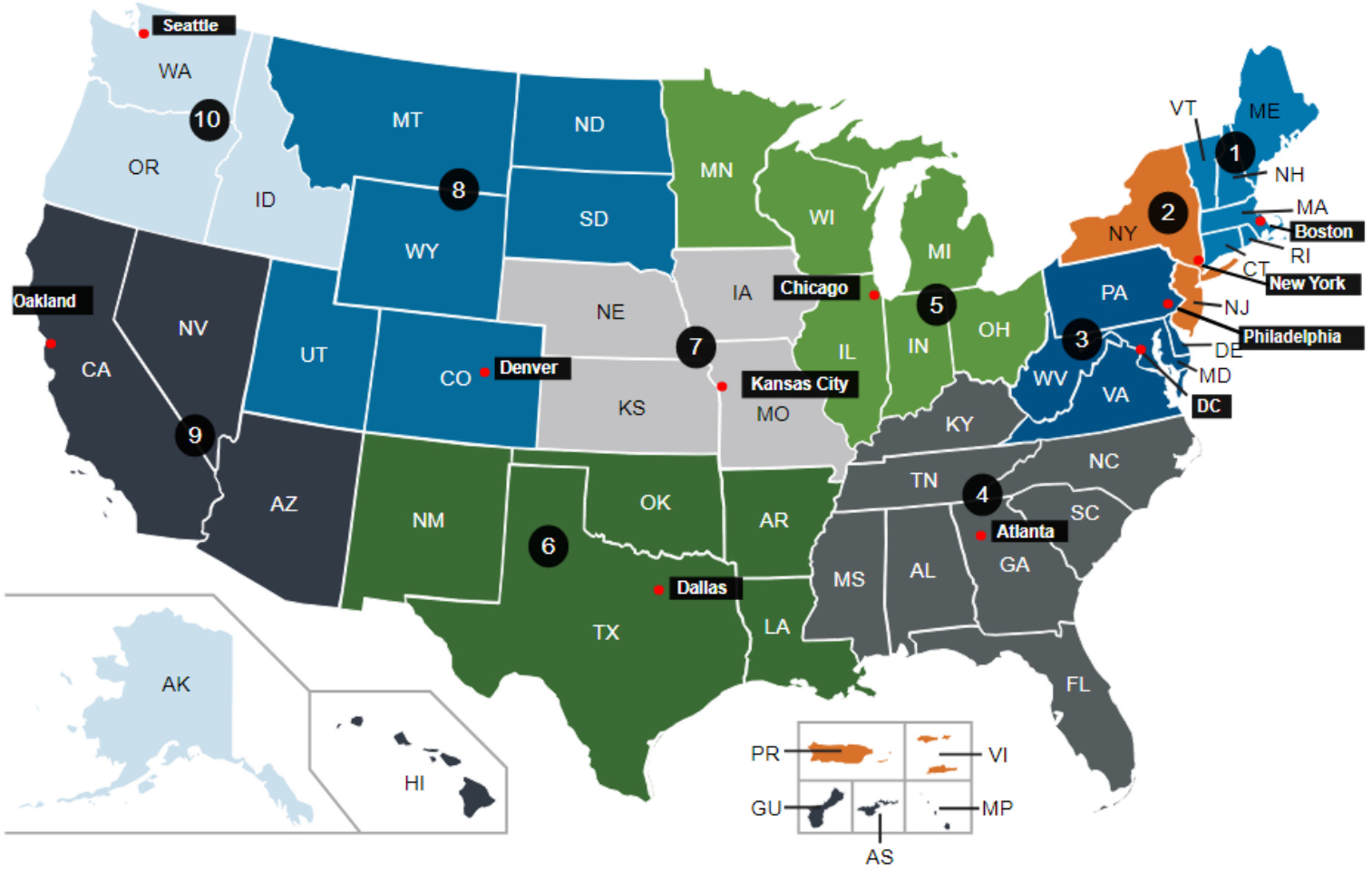
months | years | decades

Critical Infrastructure Sectors

CISA assists the public and private sectors to secure their networks and focuses on organizations in the following 16 critical infrastructure sectors.

CISA Regions

Region	Location
1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



CISA Region 6: CISARegion6@hq.dhs.gov

Cybersecurity State Coordinator Role

The role of the State Cybersecurity Coordinator is to build strategic public and private sector relationships in Texas to facilitate the development and maintenance of secure and resilient infrastructure, pursuant to 6 United States Code, Section 665(c) (2021).

- Build strategic public and private sector relationships;
- Serve as the Federal cybersecurity risk advisor;
- Facilitate the sharing of cyber threat information;
- Raise awareness of cyber resources from the Federal Government to non-Federal entities;
- Support training, exercises, and planning for continuity of operations from cyber incidents;
- Serve as a principal point of contact for non-Federal entities to engage the Federal Government on preparing, managing, and responding to cyber incidents;
- Assist State, local, Tribal, and territorial governments in development of State cyber plans;
- Coordinate with appropriate officials within the Agency (CISA).

Cybersecurity Advisors (CSAs)

To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Tribal, and Territorial (SLTT) governments.

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

Cybersecurity Resources and Services

CISA Cybersecurity Resources Snapshot

Regional Cybersecurity Resources:

- Cybersecurity Assessments (*Performed by Cybersecurity Advisors*)
  - Introductory Level:
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals Assessment (CPG)
  - Intermediate Level:
    - Cyber Infrastructure Survey (CIS)
  - Advanced Level:
    - Cyber Resilience Review (CRR)
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
- Cybersecurity Exercises and Workshops (*Performed by Cybersecurity Advisors*)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Intro to Digital Forensics Workshop (DFW)
  - Facilitated Cyber Exercise (FCE)

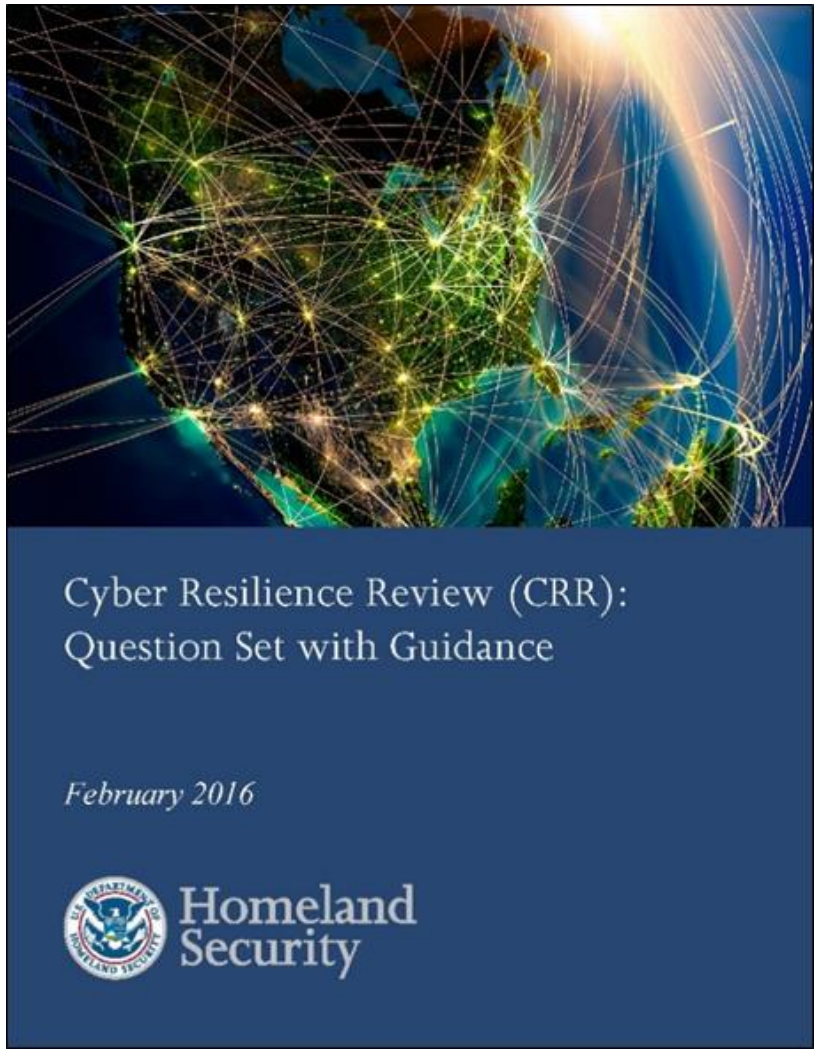
National/Automated Cybersecurity Resources:

- Vulnerability Scanning Service (CyHy)

Cybersecurity Assessments

Cyber Resilience Review (CRR)

- **Purpose**: The CRR is an assessment intended to evaluate an organization's operational resilience and cybersecurity practices of its critical services
- **Time to Complete**: ~6-8 hours
- **Delivery**: Facilitated by a CISA Cybersecurity Advisor (CSA)
- **Goal**: Helps partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk
  - Evaluates the maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities
  - Based on the CERT ® Resilience Management Model (CERT® RMM)



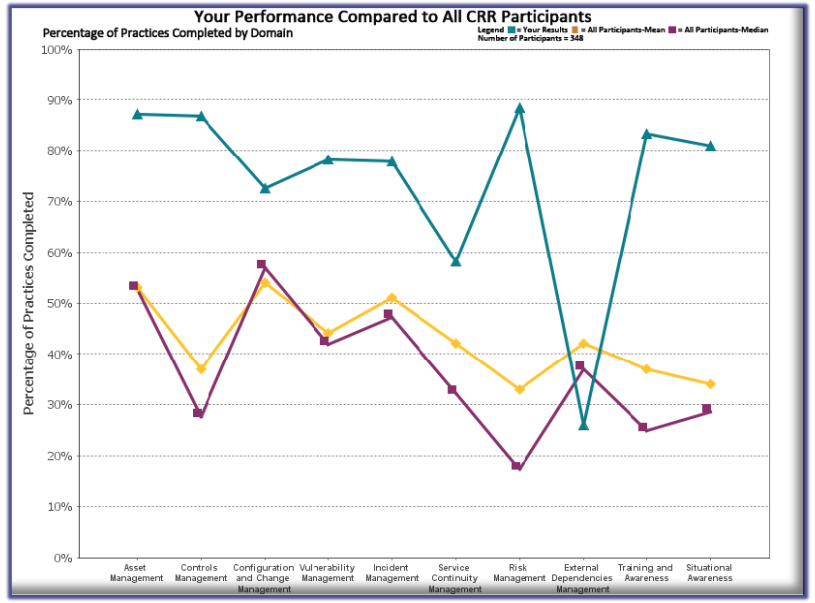
Cyber Resilience Review (CRR) | Domains

These represent key areas that typically contribute to an organization's cyber resilience— each domain focuses on:

- Documentation in place, and periodically reviewed & updated
- Communication and notification to all those who need to know
- Execution/Implementation & analysis in a consistent, repeatable manner
- Alignment of goals and practices within and across CRR domains

AM	**Asset Management** *identify, document, and manage assets during their life cycle*	SCM	**Service Continuity Management** *ensure continuity of IT operations in the event of disruptions*
CCM	**Configuration and Change Management** *ensure the integrity of IT systems and networks*	RISK	**Risk Management** *identify, analyze, and mitigate risks to services and IT assets*
CNTL	**Controls Management** *identify, analyze, and manage IT and security controls*	EXD	**External Dependency Management** *manage IT, security, contractual, and organizational controls that are dependent on the actions of external entities*
VM	**Vulnerability Management** *identify, analyze, and manage vulnerabilities*	TRNG	**Training and Awareness** *promote awareness and develop skills and knowledge*
IM	**Incident Management** *identify and analyze IT events, detect cyber security incidents, and determine an organizational response*	SA	**Situational Awareness** *actively discover and analyze information related to immediate operational stability and security*

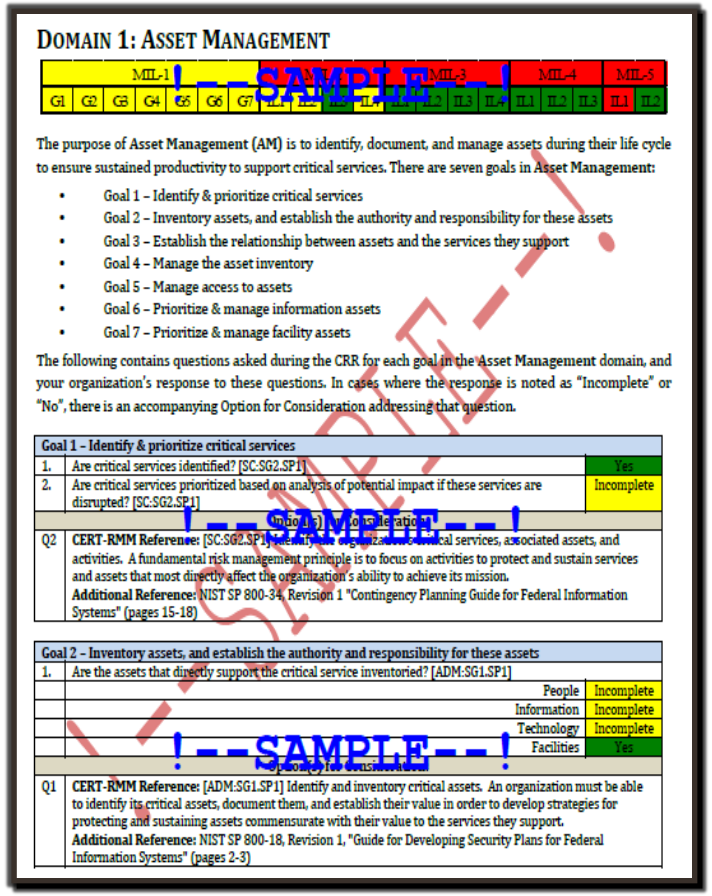
Benefits of CRR



Comparison data with other CRR participants

A summary “snapshot” graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses



DOMAIN 1: ASSET MANAGEMENT

MIL-1			MIL-2				MIL-3				MIL-4		MIL-5	
G1	G2	G3	G4	G5	G6	G7	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

The purpose of **Asset Management (AM)** is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in **Asset Management:**

- Goal 1 – Identify & prioritize critical services
- Goal 2 – Inventory assets, and establish the authority and responsibility for these assets
- Goal 3 – Establish the relationship between assets and the services they support
- Goal 4 – Manage the asset inventory
- Goal 5 – Manage access to assets
- Goal 6 – Prioritize & manage information assets
- Goal 7 – Prioritize & manage facility assets

The following contains questions asked during the CRR for each goal in the **Asset Management** domain, and your organization's response to these questions. In cases where the response is noted as "Incomplete" or "No", there is an accompanying Option for Consideration addressing that question.

Goal 1 – Identify & prioritize critical services		
1.	Are critical services identified? [SC:SG2.SP1]	Yes
2.	Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC:SG2.SP1]	Incomplete
	Option(s) for Consideration	
Q2	**CERT-RMM Reference:** [SC:SG2.SP1] Identify the organization's critical services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. **Additional Reference:** NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 15-18)	

Goal 2 – Inventory assets, and establish the authority and responsibility for these assets		
1.	Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	
	People	Incomplete
	Information	Incomplete
	Technology	Incomplete
	Facilities	Yes
	Option(s) for Consideration	
Q1	**CERT-RMM Reference:** [ADM:SG1.SP1] Identify and inventory critical assets. An organization must be able to identify its critical assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to the services they support. **Additional Reference:** NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems" (pages 2-3)	

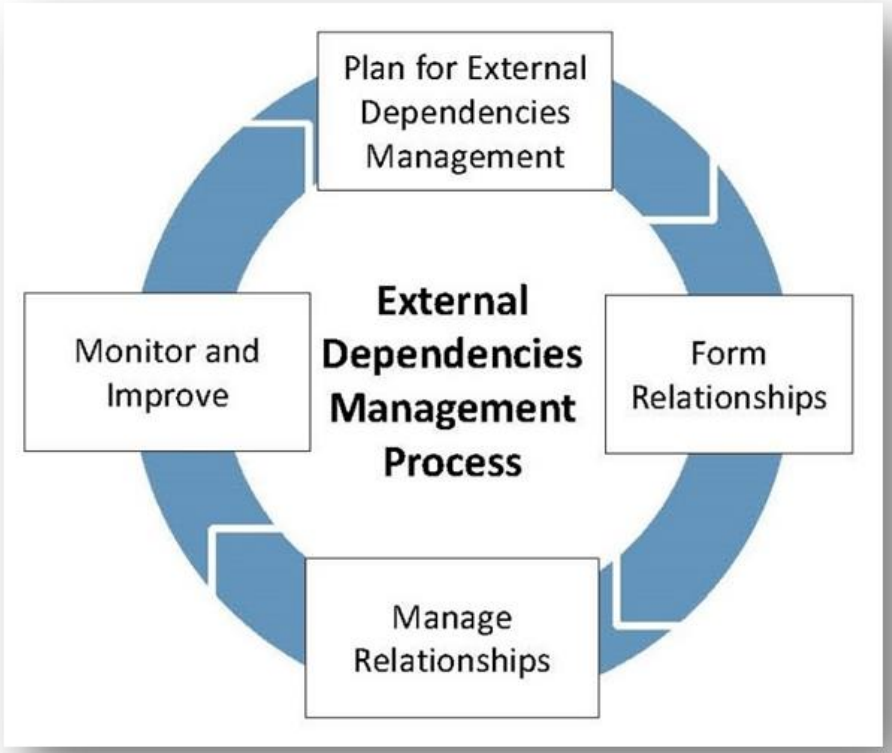
CRR Mappings to Other Frameworks

The Cyber Resilience Review has been mapped to:

- NIST Cybersecurity Framework (CSF)
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity Assessment Tool (CAT)
- NIST Special Pub 800-53 rev 4 (This mapping has not yet been published)

Most Cybersecurity Frameworks are being mapped to the NIST Cybersecurity Framework as a result that mapping can be used to indirectly map them to the CRR

External Dependency Management (EDM)



EDM process outlined in the External Dependencies Management Resource Guide

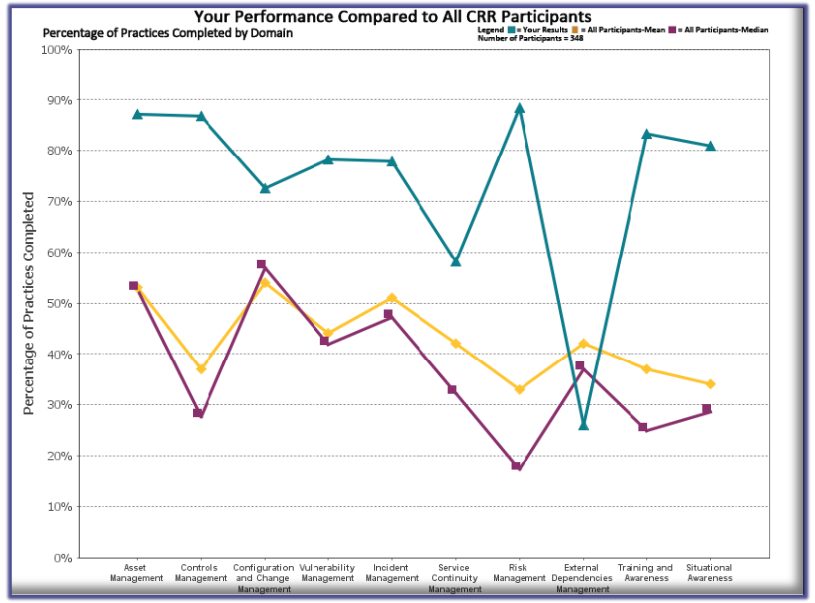
- **Purpose**: The EDM is an interview-based assessment of the management activities and practices utilized to identify, analyze, and reduce risks arising from third parties.
- **Time to Complete**: ~3-4 hours
- **Delivery**: Facilitated by a CISA Cybersecurity Advisor (CSA)
- **Benefits**:
  - The EDM Assessment measures essential external dependency cybersecurity capabilities and behaviors to provide meaningful indicators of an organization's resilience during normal operations and during times of operational stress.
  - Provides comparative data across each domain.

External Dependency Management (EDM)

To provide the organization with an understandable and useful structure for the evaluation, the EDM Assessment is divided into three distinct areas (domains):

1. **RELATIONSHIP FORMATION** – how the organization considers third party risks, selects external entities, and forms relationships with them so that risk is managed from the start
2. **RELATIONSHIP MANAGEMENT AND GOVERNANCE** – how the organization manages ongoing relationships with external entities to support and strengthen its critical services at a managed level of risk and cost
3. **SERVICE PROTECTION AND SUSTAINMENT** – how the organization plans for, anticipates, and manages disruption or incidents related to external entities

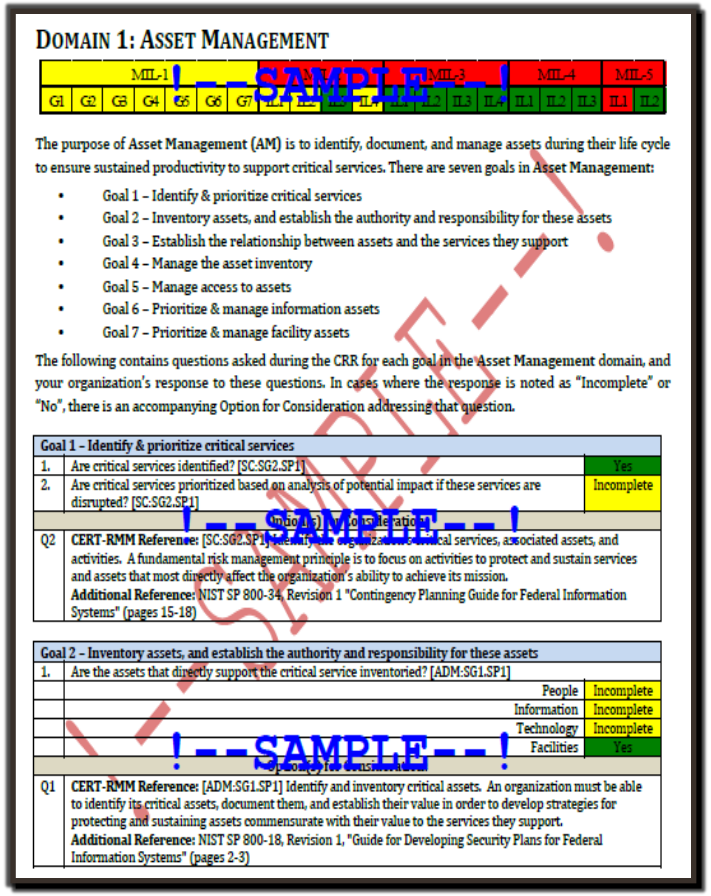
Benefits of EDM



Comparison data with other EDM participants

A summary “snapshot” graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses



DOMAIN 1: ASSET MANAGEMENT

MIL-1			MIL-2				MIL-3				MIL-4		MIL-5	
G1	G2	G3	G4	G5	G6	G7	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

The purpose of Asset Management (AM) is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in Asset Management:

- Goal 1 – Identify & prioritize critical services
- Goal 2 – Inventory assets, and establish the authority and responsibility for these assets
- Goal 3 – Establish the relationship between assets and the services they support
- Goal 4 – Manage the asset inventory
- Goal 5 – Manage access to assets
- Goal 6 – Prioritize & manage information assets
- Goal 7 – Prioritize & manage facility assets

The following contains questions asked during the CRR for each goal in the Asset Management domain, and your organization's response to these questions. In cases where the response is noted as "Incomplete" or "No", there is an accompanying Option for Consideration addressing that question.

Goal 1 – Identify & prioritize critical services		
1.	Are critical services identified? [SC:SG2.SP1]	Yes
2.	Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC:SG2.SP1]	Incomplete
	Option(s) for Consideration	
Q2	**CERT-RMM Reference:** [SC:SG2.SP1] Identify the organization's critical services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. **Additional Reference:** NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 15-18)	

Goal 2 – Inventory assets, and establish the authority and responsibility for these assets		
1.	Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	
	People	Incomplete
	Information	Incomplete
	Technology	Incomplete
	Facilities	Yes
	Option(s) for Consideration	
Q1	**CERT-RMM Reference:** [ADM:SG1.SP1] Identify and inventory critical assets. An organization must be able to identify its critical assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to the services they support. **Additional Reference:** NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems" (pages 2-3)	

Cybersecurity Workshops & Exercises

Incident Management Workshop (IMW)

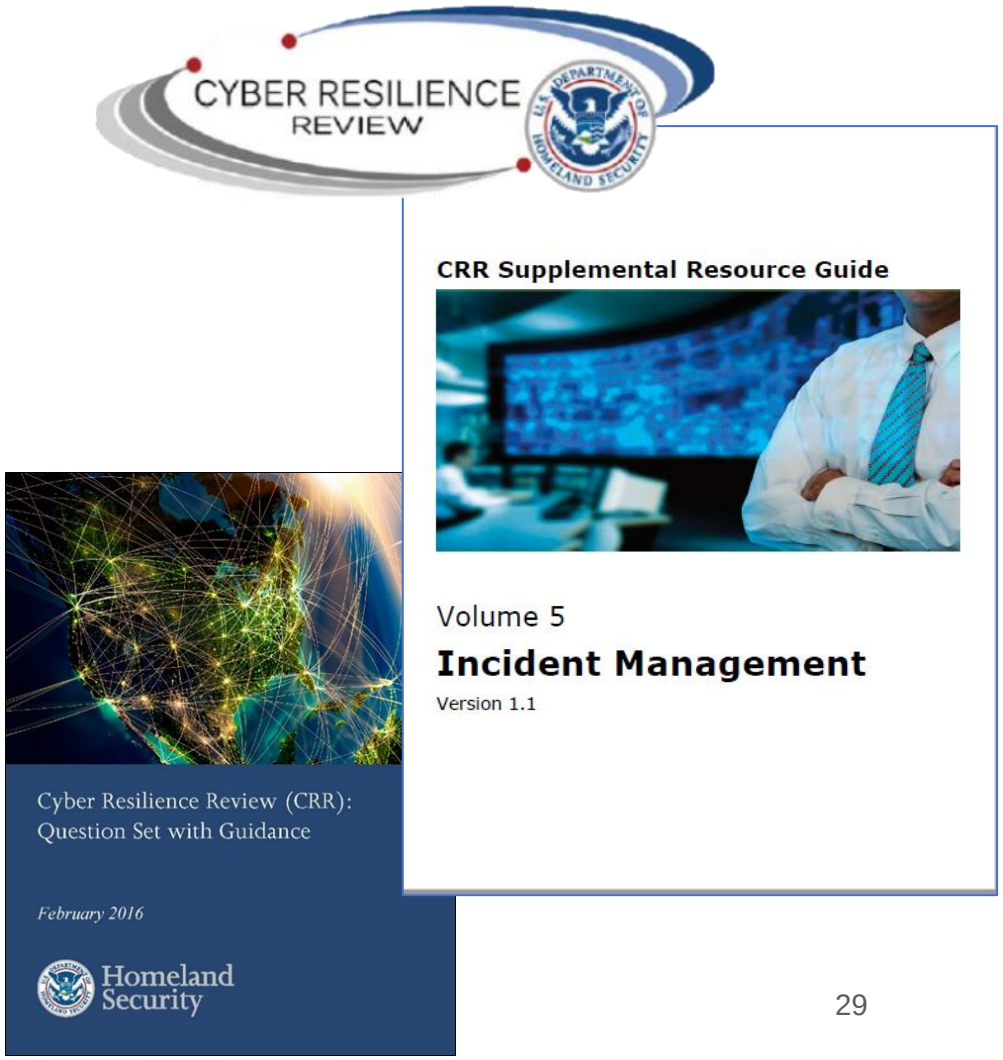
Description: A 2-hour non-technical and informative session designed to help organizations understand incident management concepts, key elements, planning and implementation.

Goal: The goal of the workshop is to provide organizations with tangible, useful takeaway information on how to manage cybersecurity incidents effectively and, ultimately, achieve operational resilience.

Audience: Organizations that want to learn about an approach to developing a cyber incident management capability.

Format:

In-Person or Virtual



Facilitated Cyber Exercise (FCE)

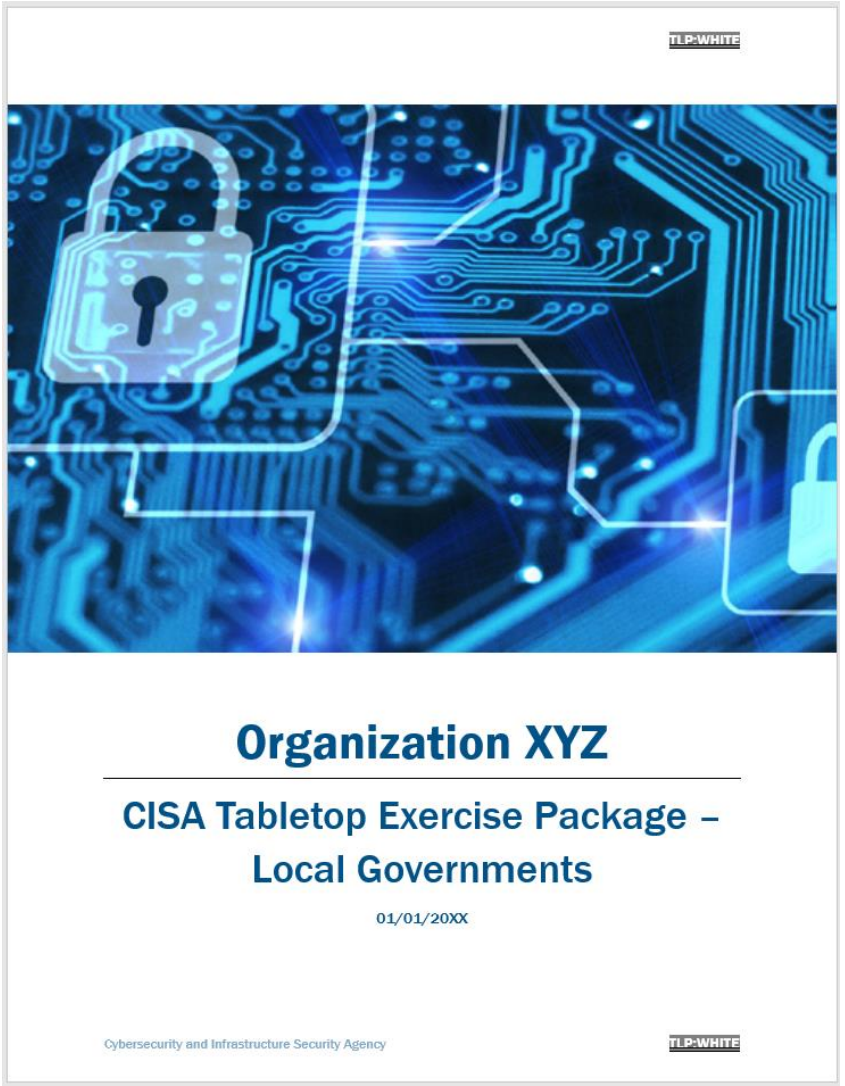
Description: A 2-hour or 4-hour non-technical facilitated cybersecurity tabletop exercise, where organizations are presented with a cyber threat-based scenario and are challenged to consider how their organization would respond, based on existing incident response plans.

Goal: The goal of the workshop is to provide organizations an opportunity to assess their level of readiness to respond to and recover from a cybersecurity incident impacting their operating environment.

Audience: Organizations that want to assess their level of readiness to respond to and recover from a cybersecurity incident.

Format:

In-Person or Virtual



National Resources

Cyber Hygiene Services

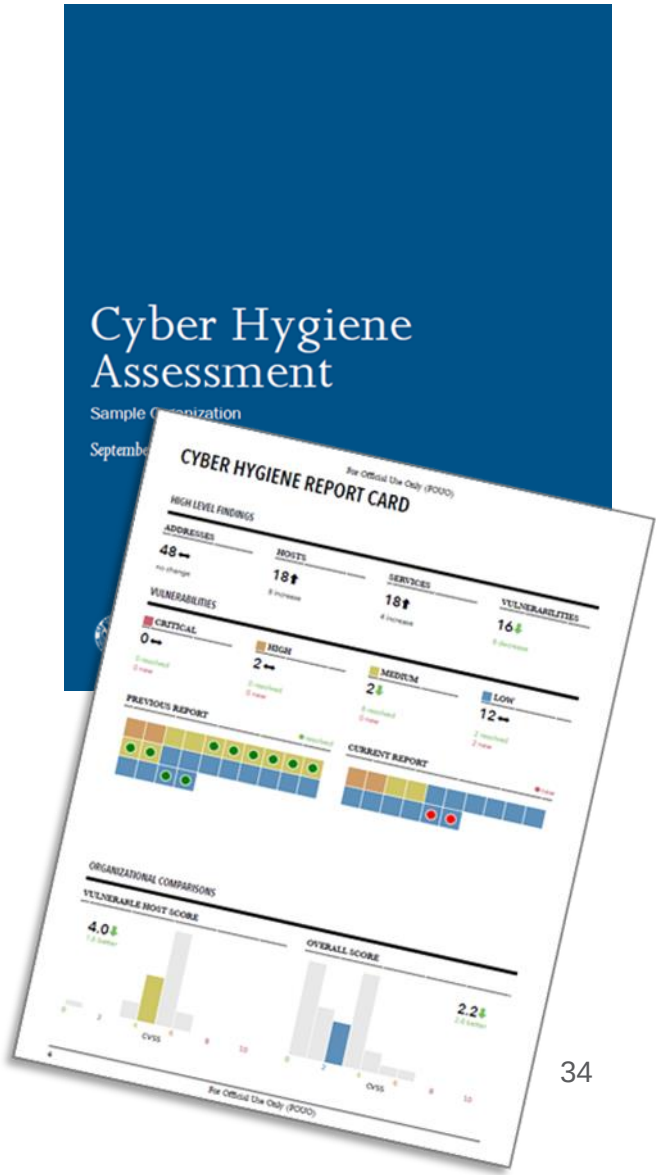
Vulnerability Scanning Service (CyHy)

Assess Internet accessible systems for known vulnerabilities and configuration errors

Work with organization to proactively mitigate threats and risks to systems

Activities include:

- Network Mapping
  - Identify public IP address space
  - Identify hosts that are active on IP address space
  - Determine the O/S and Services running
  - Re-run scans to determine any changes
  - Graphically represent address space on a map
- Network Vulnerability & Configuration Scanning
  - Identify network vulnerabilities and weakness



Information Sharing and Awareness

National Cyber Awareness System

The National Cyber Awareness System offer a variety of information for users with varied technical expertise. Those with more technical interest can read the Alerts, Analysis Reports, Current Activity, or Bulletins. Users looking for more general-interest pieces can read the Tips.

A subscription to any or all of the National Cyber Awareness System products ensures that you have access to timely information about security topics and threats. To learn more or to subscribe, visit the subscription system.

https://www.cisa.gov/uscert/ncas

Current Activity

Provides up-to-date information about high-impact types of security activity affecting the community at large.

View Current Activity

Alerts

Provide timely information about current security issues, vulnerabilities, and exploits.

View Alerts

Bulletins

Provide weekly summaries of new vulnerabilities. Patch information is provided when available.

View Bulletins

Analysis Reports

Provide in-depth analysis on a new or evolving cyber threat.

View Analysis Reports

Cybersecurity Education & Training Resources

Federal Virtual Training Environment (FedVTE)

Cyber professionals can continue to improve their skills through hands-on training opportunities.

FedVTE is an online, on-demand training center that provides free cybersecurity training for federal, state, local, tribal, and territorial government employees and to U.S. veterans.

Example Content:

- Cloud Computing Security
- Cloud Security - What Leaders Need to Know
- Cryptocurrency for Law Enforcement for the Public
- Cyber Supply Chain Risk Management for the Public
- Cyber-essentials
- Understanding DNS Attack
- Understanding Web and Email Server Security
- Don’t Wake Up to a Ransomware Attack
- Foundations of Cybersecurity for Managers
- Fundamentals of Cyber Risk Management
- Introduction to Cyber Intelligence
- Securing Internet-Accessible Systems
- 101 Coding for the Public
- 101 Reverse Engineering for the Public

https://fedvte.usalearning.gov

Cybersecurity Incident Reporting

Phishing and Incident Reporting / Malware Analysis

24x7 contact number: 888-282-0870 | central@cisa.dhs.gov

Report Phishing to: phishing-report@us-cert.gov

CISA partners with the Anti-Phishing Working Group (APWG) to collect phishing email messages and website locations to help people avoid becoming victims of phishing scams.

Where/How/When to Report Incidents: https://www.cisa.gov/forms/report

If there is a suspected or confirmed cyber attack or incident that affects core government or critical infrastructure functions and/or results in the loss of data, system availability or control of systems.

Advanced Malware Analysis Center: https://malware.us-cert.gov

Provides 24x7 dynamic analyses of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining the results of the analysis. Experts will detail recommendations for malware removal and recovery activities.

Next Steps: Cybersecurity Partnership Formation

Next Steps: Cybersecurity Partnership Formation

Would you like to partners with CISA and leverage our no-cost cybersecurity assessments, workshops, education, training, and information sharing resources?

Next Steps:

1. Visit https://www.cisa.gov/cisa-regions; and
2. Contact your CISA Regional Office and request an initial briefing with your Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA).

44

CISA's Election Security Services

CISA's services are available at no cost to state and local government officials and private sector election infrastructure partners. All services are available upon request and are strictly voluntary; CISA only provides services when requested and does not disclose with which stakeholders it works.

Key areas of our services are included in the links below:

- **Cybersecurity Assessments**, such as Cyber Hygiene Vulnerability Scanning and Cyber Resilience Reviews.
- **Detection and Prevention**, such as Cyber Threat Hunting and Enhanced Cyber Services.
- **Exercises**, such as tabletops, providing stakeholders with mechanisms to examine plans and procedures, identifying areas for improvement, sharing best practices, and enhancing preparedness against threats to election infrastructure, including cyber incidents and physical threats such as civil unrest or threats to election officials.
- **Incident Response**, provides 24/7 intrusion analysis in response to cyber incidents.
- **Information Sharing and Awareness**, such as the National Cyber Awareness System alerts and advisories, and the Homeland Security Information Network portal.
- **Regional Directors, Cybersecurity Advisors, and Protective Security Advisors** are regionally located personnel who offer state and local governments, as well as private sector partners, immediate and sustained assistance, coordination, and outreach to prepare for and protect from cyber and physical threats.
- **Training and Career Development**, including **CISA's election security trainings**, and National Initiative for Cybersecurity Careers and Studies Catalog.

https://www.cisa.gov/election-security-services

45

CISA REGION 6

Ernesto Ballesteros, JD, MS, CISSP, CISA, Security+

Cybersecurity State Coordinator of Texas, Region 6
Cybersecurity & Infrastructure Security Agency

EMAIL: ernesto.ballesteros@cisa.dhs.gov
CELL: (210) 202-6646

CISA Region 6
CISARegions6@hq.dhs.gov

CISA CENTRAL - 24/7 Watch
(888) 282-0870;Central@cisa.dhs.gov

FBI's 24/7 Cyber Watch (CyWatch)
(855) 292-3937; CyWatch@fbi.gov