

INTRO AND OVERVIEW

CYBER STATS

CYBER THREATS

AWARENESS, PREPAREDNESS & RESILIENCE

DHS/CISA SERVICES & TOOLS

SUMMARY & Q&A

CLOSING



CYBER STATS, UPDATE AND THREATS

Gatewood
CSC/CSA
Cybersecurity and Infrastructure Security Agency

19 March 2023



Cyber Stats, Threats and Updates

January 1, 1983, is considered the official birthday of the Internet. Prior to this, the various computer networks did not have a standard way to communicate with each other. A new communications protocol was established called Transfer Control Protocol/Internet Protocol (TCP/IP).

University System of Georgia

ARPANET initially connected four independent network nodes situated at University of California, Los Angeles (UCLA), Stanford Research Institute (SRI), the University of California-Santa Barbara (UCSB) and the University of Utah.

University System of Georgia

“As of January 2023, there were 5.16 billion internet users worldwide, which is 64.4 percent of the global population. Of this total, 4.76 billion, or 59.4 percent of the world's population, were social media users.”

Statista 2023

“According to Cybersecurity Ventures, the cost of cybercrime is predicted to hit \$8 trillion in 2023 and will grow to \$10.5 trillion by 2025.”

Forbes 2023



Cyber Stats, Threats and Updates

1. Ransomware
2. E-Mail
3. Vulnerability in the cloud
4. State sponsored threats
5. Mobile attacks
6. Critical infrastructure attacks/Internet-of-Things attacks
7. An alarming shortage of cybersecurity professionals (Knowledge + Skills + Abilities + Experience)
8. Hybrid or remote work environments
9. Cyber-Physical attacks
10. 3rd party vulnerabilities (vendors, contractors, partners)



Cyber Stats, Threats and Updates

- 6 attack entities:
 - Healthcare industry
 - Government (SLTT)
 - Financial services
 - Energy and utilities
 - Supply chain
 - YOU!
 - Social networking
 - Conferences
 - Travel sites
 - ...



FEAR/UNCERTAINTY/DOUBT – OH MY...

Can we protect, defend, work, play and live in cyberspace?

19 March 2023



Can we protect, defend, work, play and live in cyberspace?

YES!

Cybersecurity is a “sweet combination of physical + logical and human-element” security...

Cybersecurity is a team-sport

Cybersecurity: Awareness + Preparedness + Resilience



Focus on...

Known knowns, “things we know we know”

Known unknowns, "some things we do not know"

Unknown unknowns, “things we don’t know we don’t know.

“Donald H. Rumsfeld – Secretary of Defense”



Awareness + Preparedness + Resilience

- Awareness

- User awareness:

- User awareness is **knowledge that leads to appropriate security behaviors**. Knowledge itself is insufficient, true awareness requires that people behave in accordance with that knowledge.
 - Awareness, training and education
 - Rules of Behavior and/or Appropriate Use Policy
 - Testing
 - Exercising (TTX)
 - Pen-Testing
 - Vulnerability Scanning



Awareness

- Situational Awareness:
 - Situational awareness can be defined simply as “**knowing what is going on around us...**”
 - Examples are **awareness of uncertain assumptions, awareness of activities**, ability to focus awareness on important factors, and active seeking of confirming/disconfirming evidence.
- Aspects/Areas of Focus of situation awareness:
 - Network Awareness
 - Threat Awareness
 - Mission Awareness

Levels: Tactical & Operational Awareness



Preparedness

- **Preparedness**

- Cyber preparedness requires testing our plans, ongoing monitoring, analysis, and annual exercises:
 - Cyber Governance, Cyber Policies/Standards, Compliance Management, Risk Management, Cyber Incident Response/Handling/Management, Security Awareness, Continuity of Operations (backups & recovery, IR, DRP/BCP, CMMC)

Preparedness is “left of bang” ...



Focus...

Read and study “Left of Bang/Boom”:

The strategy of putting controls in place to mitigate potential threats before systems can be compromised has been described as “moving left”. It can also be described as “Left of Boom” cybersecurity, wherein **the 'boom' represents an incident.**



Resilience...

- **Resilience** is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.
 - In a nutshell: Proactive stance (SSP), Backups & Recovery, Incident Response/Handling/Management, DRP/BCP/Business Resumption

Resilience is “right of bang...”



Bottomline: Awareness, Preparedness and Resilience

1. Conduct a “risk assessment” or “Cyber Resilience Review” or CMMC assessment. Why?
2. Inventory and Control: All Enterprise Assets
3. Protect the Information/Data/Systems (Physical, Logical and Human Element)
4. Secure Configuration for all Assets
5. Account Management
6. Access Control
7. Backups and Recovery Management
8. Cyber Incident Management/Handling/Reporting
9. DRP/BCP/Business Resumption
10. See Step #1



END OF PART 1 OF 2



CYBERSECURITY SERVICES FOR BUILDING CYBER RESILIENCE

Gatewood
CSC/CSA
Cybersecurity and Infrastructure Security Agency

19 March 2023

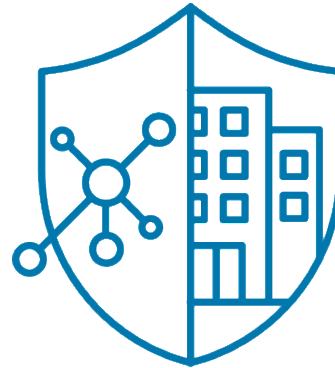


WHO WE ARE



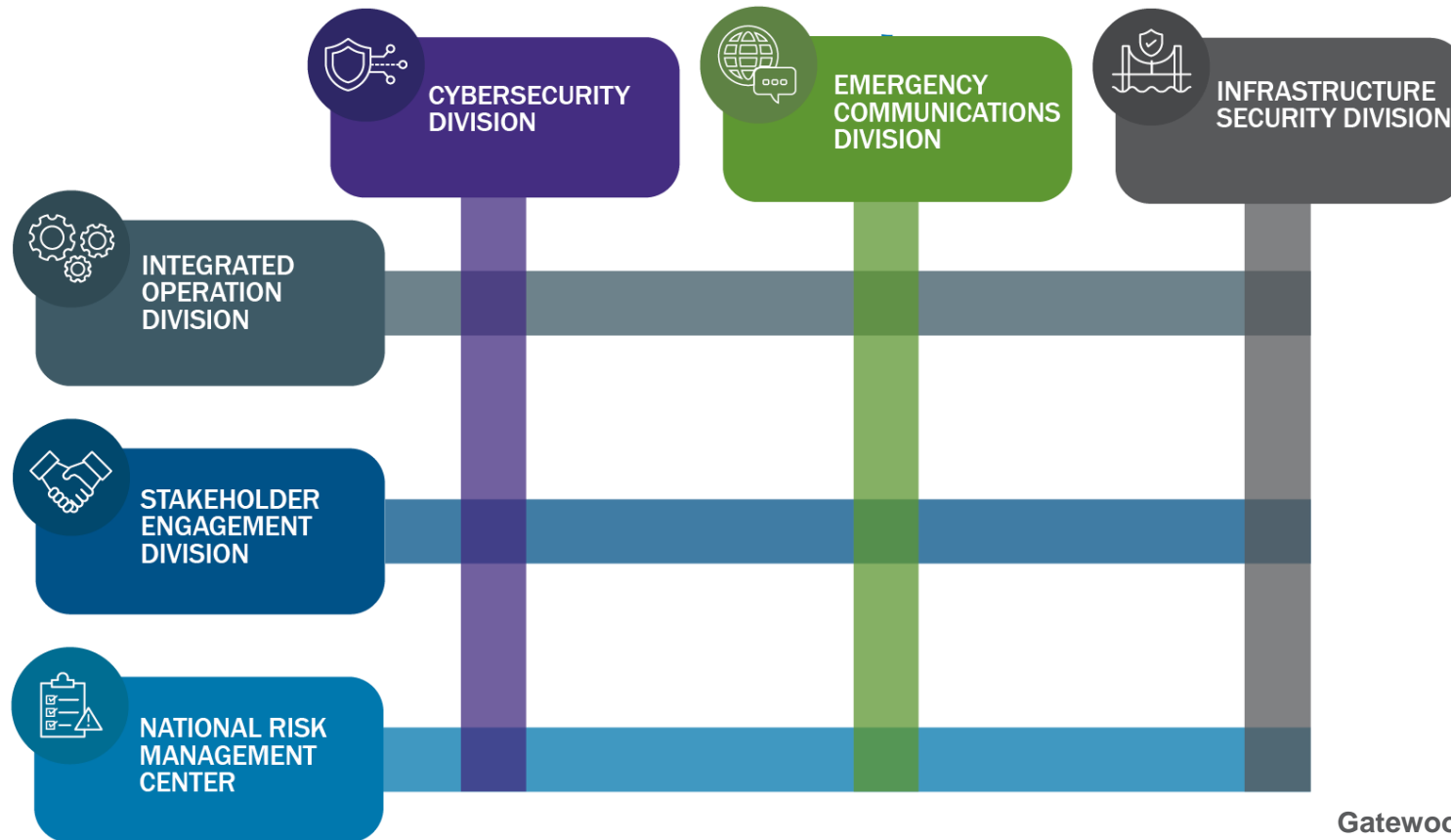
CISA Mission and Vision

- Cybersecurity and Infrastructure Security Agency (CISA) mission:
 - Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure
- CISA vision:
 - A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive



CISA in Brief

- CISA consists of:



CYBERSECURITY ADVISOR PROGRAM



Cybersecurity Advisor Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

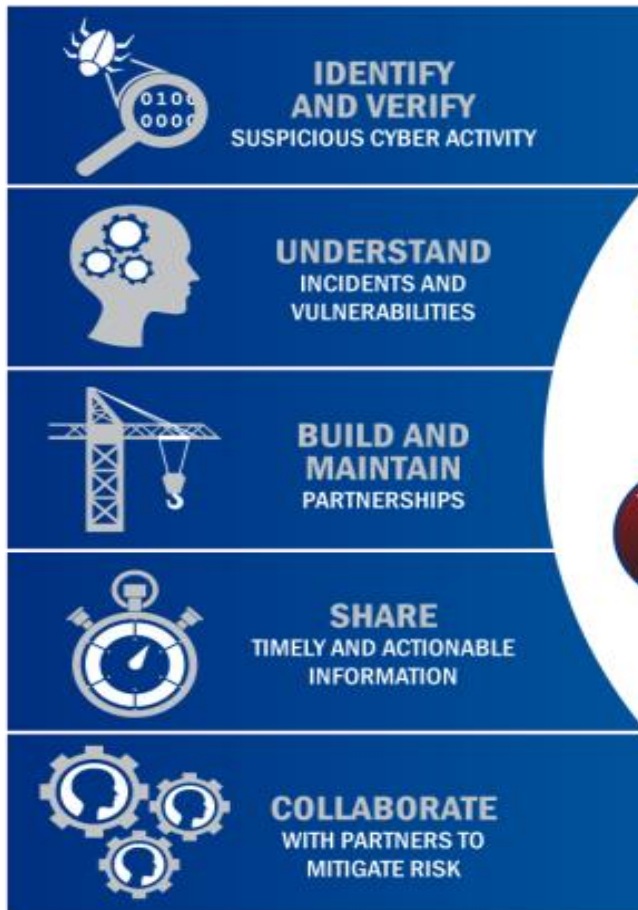
In support of that mission: Cybersecurity Advisors (CSAs):

- **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.



Serving Critical Infrastructure

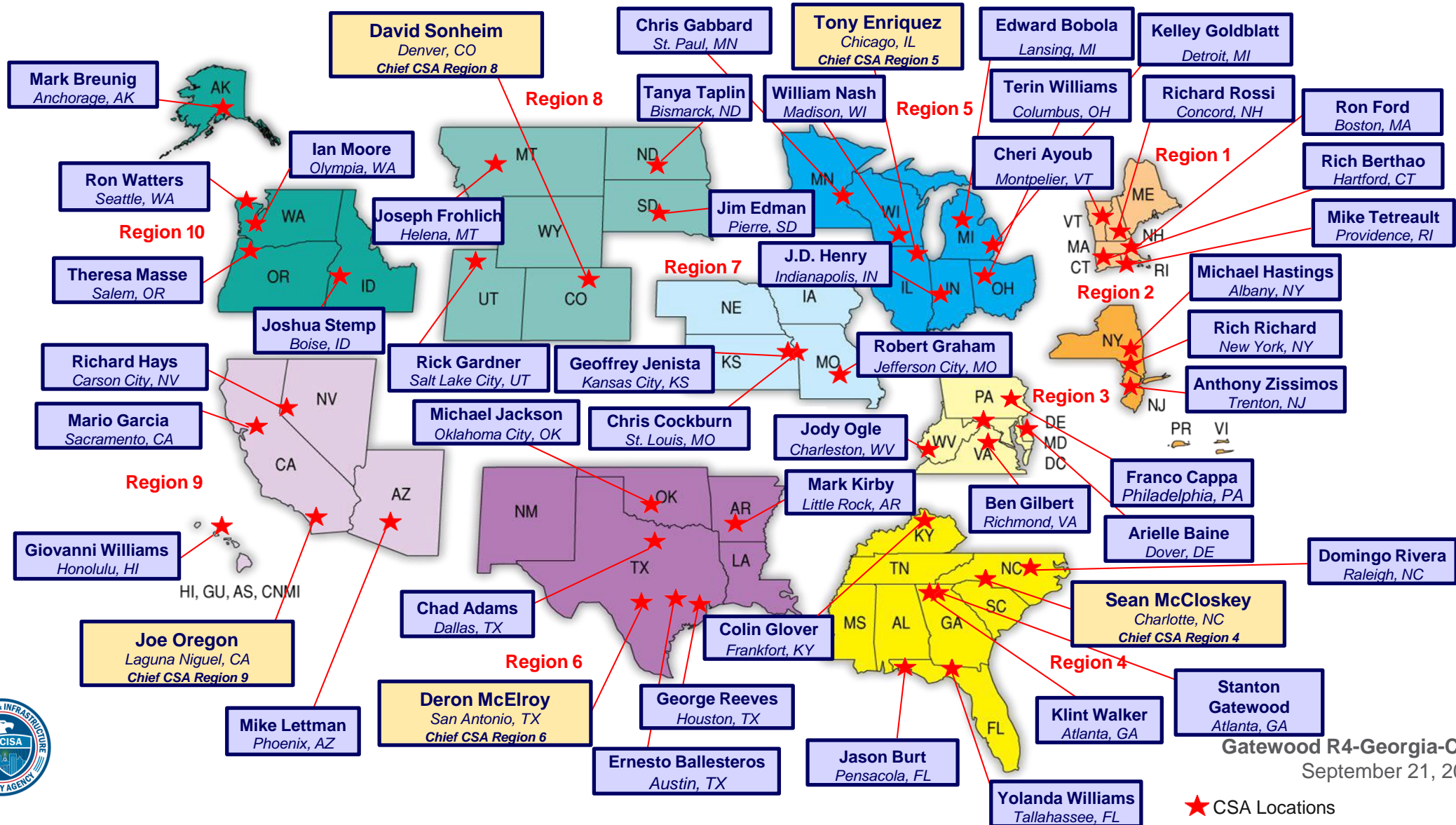
KEY ACTIVITIES:



16 CRITICAL INFRASTRUCTURE SECTORS:



CSA Deployed Personnel



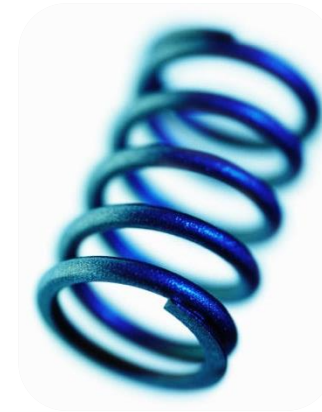
CYBERSECURITY AND RESILIENCE



Resilience Defined

“... the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents...”

- Presidential Policy Directive 21
February 12, 2013



| | |
|-----------------------------|-----------------------------|
| Protect (Security) | Sustain (Continuity) |
| Perform (Capability) | Repeat (Maturity) |



Operational Resilience in Practice

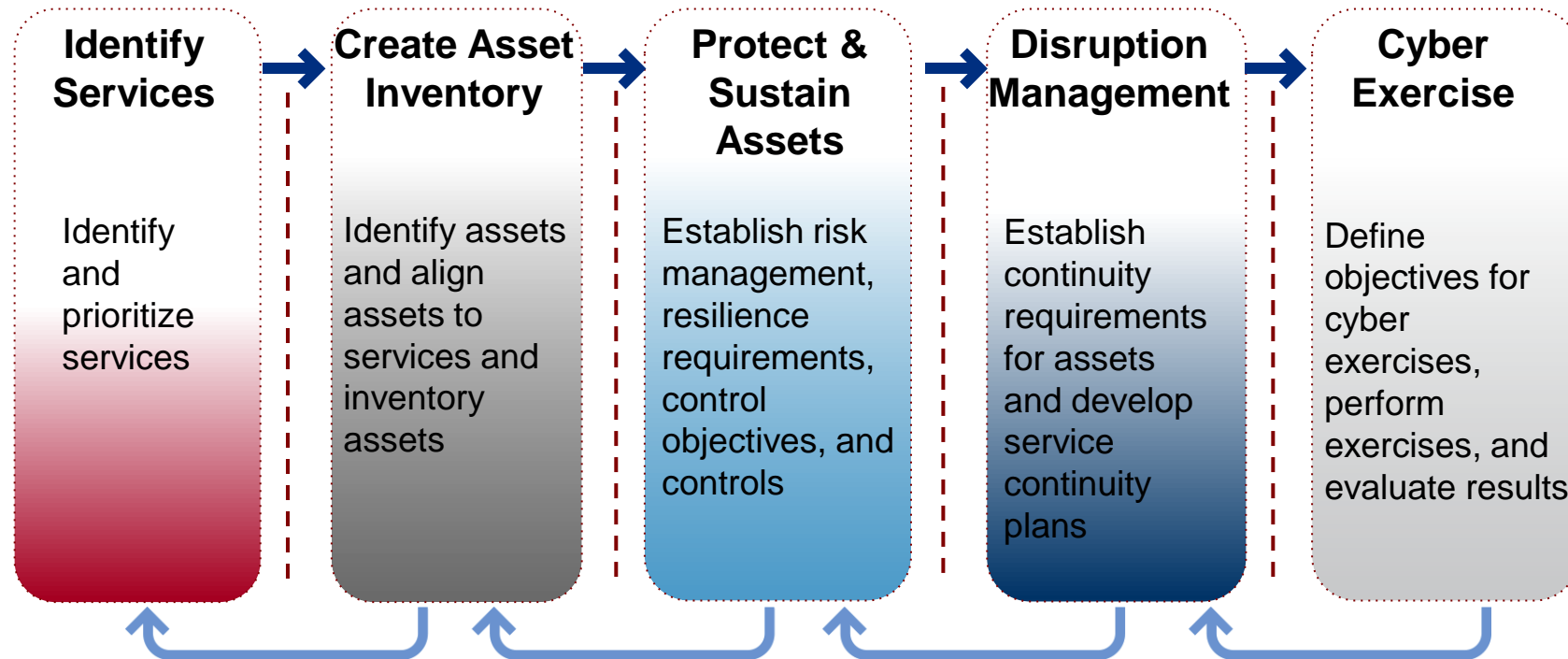
Operational resilience emerges from what we do, such as:

- Identifying and mitigating risks,
- Planning for and managing vulnerabilities and incidents,
- Performing service-continuity processes and planning,
- Managing IT operations,
- Managing, training, & deploying people,
- Protecting and securing important assets, and
- Working with external partners.



Working toward Cyber Resilience

- Follow a framework or general approach to cyber resilience. One successful approach includes:



Process Management and Improvement

CISA CYBERSECURITY SERVICES



Cybersecurity Services for All

- Cybersecurity Advisors
- State, Local, Tribal, and Territorial engagements
- Cyber Resilience Reviews (CRR™)
- External Dependencies Management (EDM) Assessments
- Cyber Infrastructure Surveys
- Cyber Education and Awareness
- Federal Virtual Training Environment (Fed VTE)
- National Initiative for Cybersecurity Careers and Studies (NICCS)
- Stop. Think. Connect.™



CISA Central

CISA Central is CISA's hub for staying on top of threats and emerging risks to our nation's critical infrastructure, whether they're of cyber, communications or physical origin:

CYBER RESOURCE HUB

- RVA Mapped to the MITRE ATT&CK Framework Infographic
- Vulnerability Scanning
- Phishing Campaign Assessment
- Risk and Vulnerability Assessment
- Cyber Resilience Review (CRR)
- CRR Downloadable Resources
- External Dependencies Management Assessment (EDM)
- EDM Downloadable Resources
- Cyber Infrastructure Survey
- Remote Penetration Testing
- Web Application Scanning
- Cyber Security Evaluation Tool (CSET®)
- Validated Architecture Design Review (VADR)



Sampling of Cybersecurity Offerings

- **Preparedness Activities**

- Information / Threat Indicator Sharing
- Cybersecurity Training and Awareness
- Cyber Exercises and “Playbooks”
- National Cyber Awareness System
- Vulnerability Notes Database
- Information Products and Recommended Practices
- Cybersecurity Evaluations
 - Cyber Resilience Reviews (CRR™)
 - Cyber Infrastructure Surveys
 - Phishing Campaign Assessment
 - Vulnerability Scanning
 - Risk and Vulnerability Assessments (aka “Pen” Tests)
 - External Dependencies Management Reviews
 - Cyber Security Evaluation Tool (CSET™)
 - Validated Architecture Design Review (VADR)

- **Response Assistance**

- Remote / On-Site Assistance
- Malware Analysis
- Hunt and Incident Response Teams
- Incident Coordination

- **Cybersecurity Advisors**

- Assessments
- Working group collaboration
- Best Practices private-public
- Incident assistance coordination

- **Protective Security Advisors**

- Assessments
- Incident liaisons between government and private sector
- Support for National Special Security Events



ASSESSMENTS

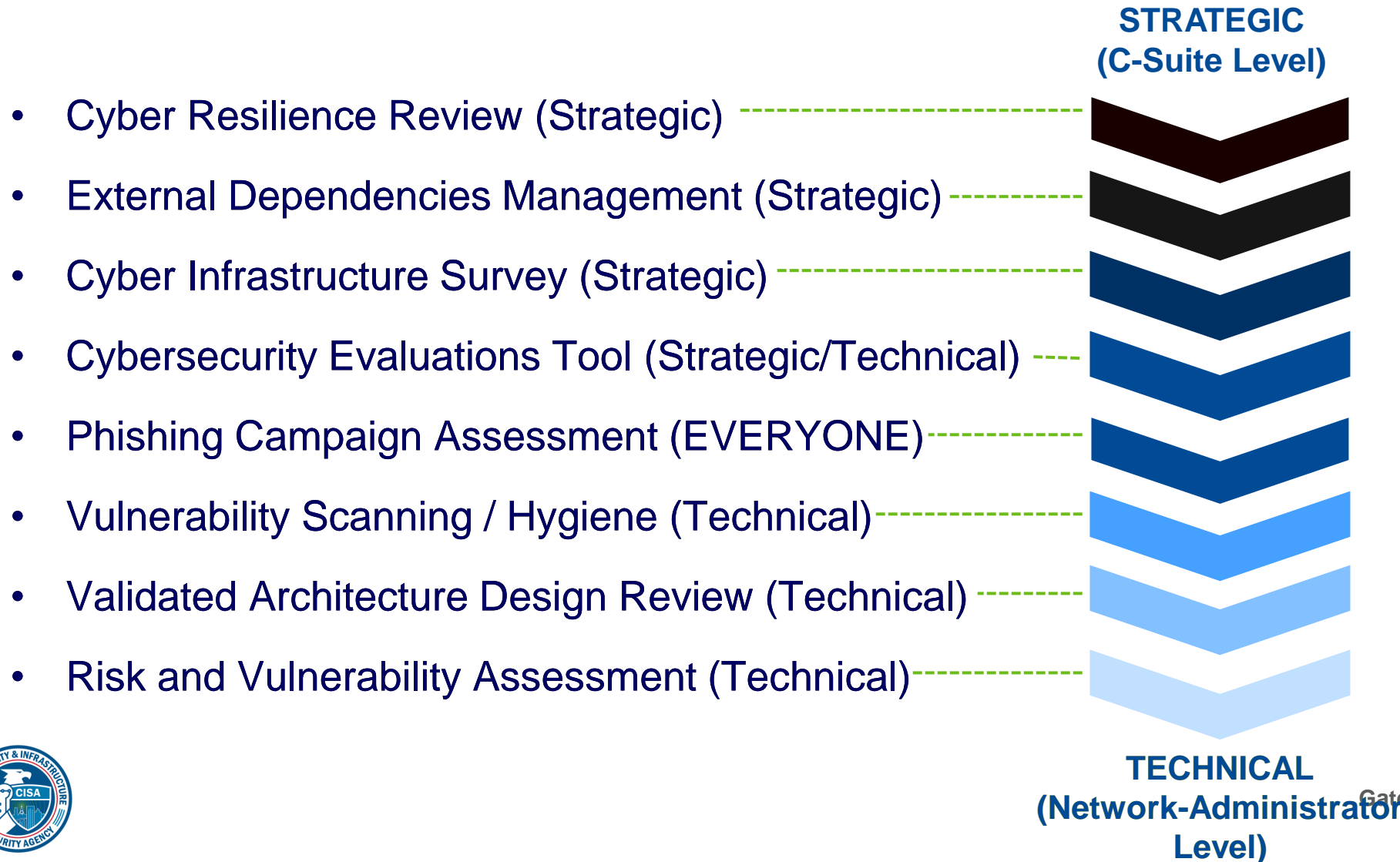


Criticality of Periodic Assessments

- Periodic assessments are essential for resilience
- Can't protect if you don't know what needs protection
- Can't fix what needs if you don't know what's wrong



Range of Cybersecurity Assessments



Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
 - Public release under Freedom of Information Act requests,
 - Public release under State, local, tribal, or territorial disclosure laws,
 - Use in civil litigation and
 - Use in regulatory purposes.



CYBER RESILIENCE REVIEW



Cyber Resilience Review

- **Purpose:** Evaluates that maturity of an organization’s capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across the following 10 domains:

| | |
|-------------------------------------|--------------------------------|
| Asset Management | Service Continuity Management |
| Controls Management | Risk Management |
| Configuration and Change Management | External Dependency Management |
| Vulnerability Management | Training and Awareness |
| Incident Management | Situational Awareness |

- Benefits include: Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



CYBER RESILIENCE REVIEW (CRR)

Question Set with Guidance

April 2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Cyber Resilience Review Domains

Asset Management

Know your assets being protected & their requirements, e.g., CIA

Risk Management

Know and address your biggest risks that considers cost and your risk tolerances

Configuration and Change Management

Manage asset configurations and changes

Service Continuity Management

Ensure workable plans are in place to manage disruptions

Controls Management

Manage and monitor controls to ensure they are meeting your objectives

Situational Awareness

Discover and analyze information related to immediate operational stability and security

External Dependencies Management

Know your most important external entities and manage the risks posed to essential services

Training and Awareness

Ensure your people are trained on and aware of cybersecurity risks and practices

Incident Management

Be able to detect and respond to incidents

Vulnerability Management

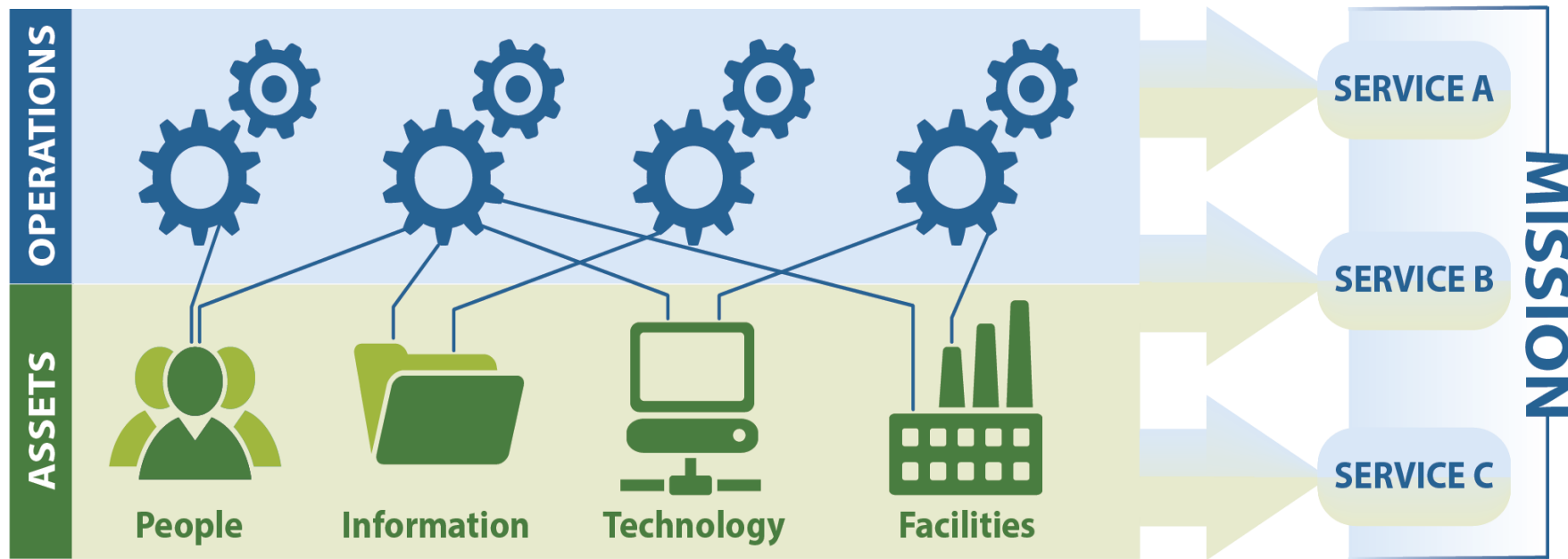
Know your vulnerabilities and manage those that pose the most risk



For more information: <https://www.cisa.gov/cisa-cybersecurity-resources>

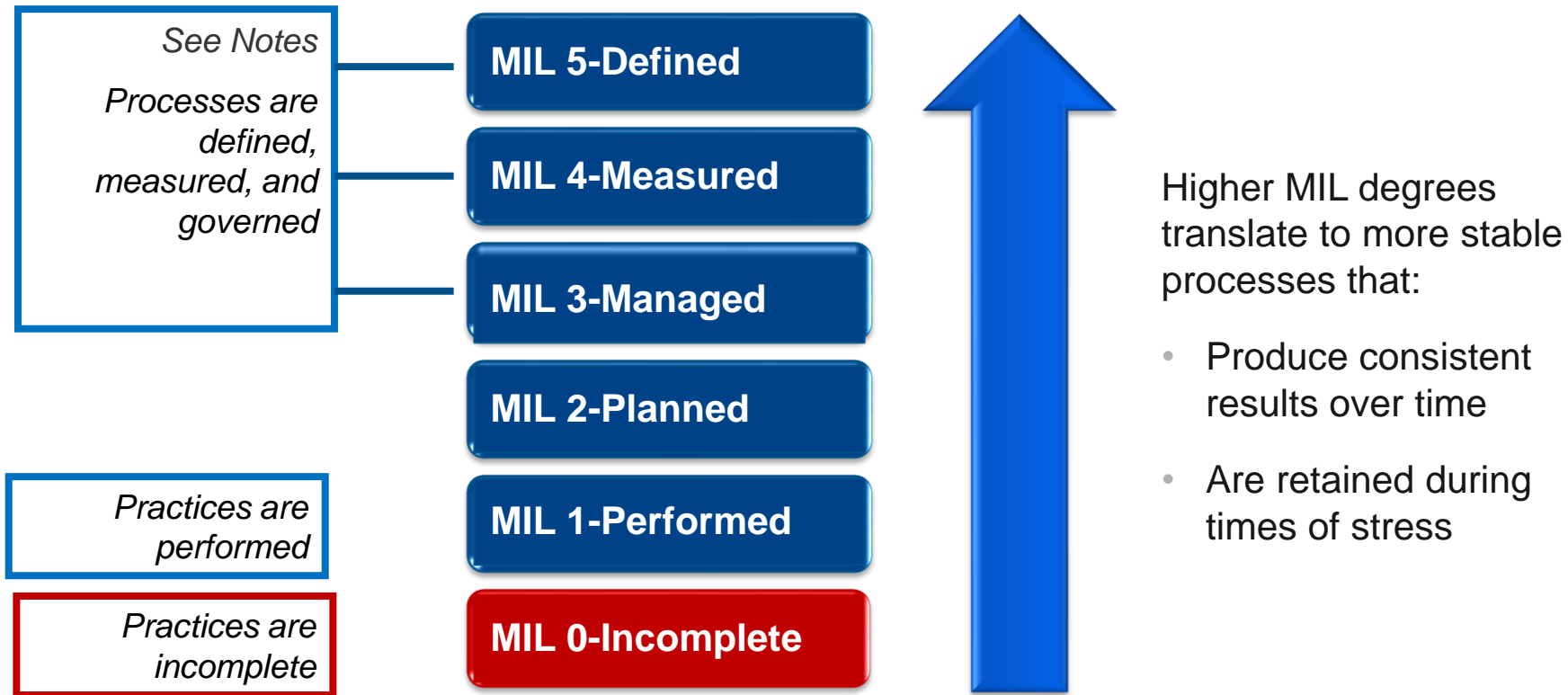
Critical Service Focus

Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions**.



Process Institutionalization

CRR maturity indicator levels (MILs) are to measure process institutionalization:

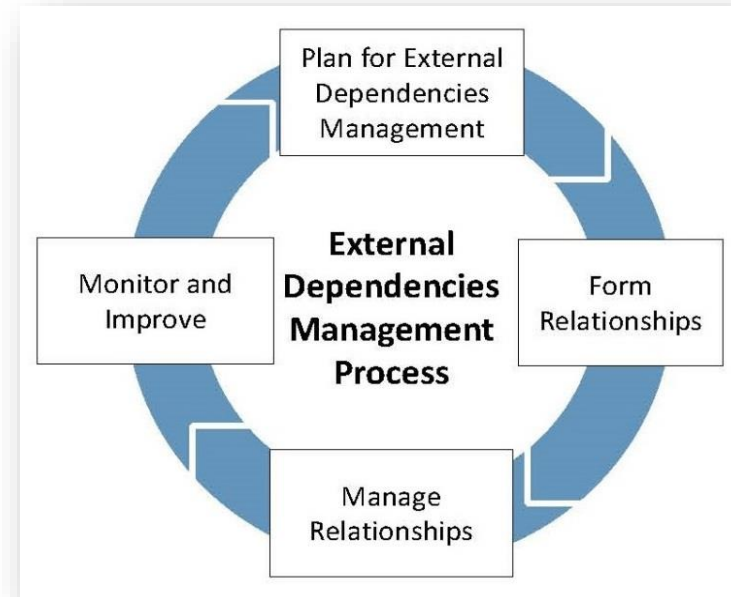


EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENTS



External Dependencies Management Assessment

- **Purpose:** Evaluate an entity's management of their dependencies on third-party entities
- **Delivery:** CSA-facilitated
- **Benefits:**
 - Better understanding of the entity's cyber posture relating to external dependencies
 - Identification of improvement areas for managing third parties that support the organization



EDM process outlined per the External Dependencies Management Resource Guide

Note: graphic edits will need time to be recreated and adjusted.

Gatewood R4-Georgia-CSA
September 21, 2023



EDM Assessment Organization and Structure

- ❑ Structure and scoring similar to Cyber Resilience Review
- ❑ Uses one Maturity Indicator Level (MIL) scale with three lifecycle domains.

Relationship Formation

Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.

Relationship Management and Governance

Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk.

Service Protection and Sustainment

Assesses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.



CYBER INFRASTRUCTURE SURVEY



Cyber Infrastructure Survey Highlights

- Purpose: Evaluate security controls, cyber preparedness, overall resilience.
- Delivery: CSA-facilitated
- Benefits:
 - Effective assessment of cybersecurity controls in place for a critical service,
 - Easy-to-use interactive dashboard to support cybersecurity planning and resource allocation), and
 - Access to peer performance data visually depicted on the dashboard.



Example of CIS Dashboard

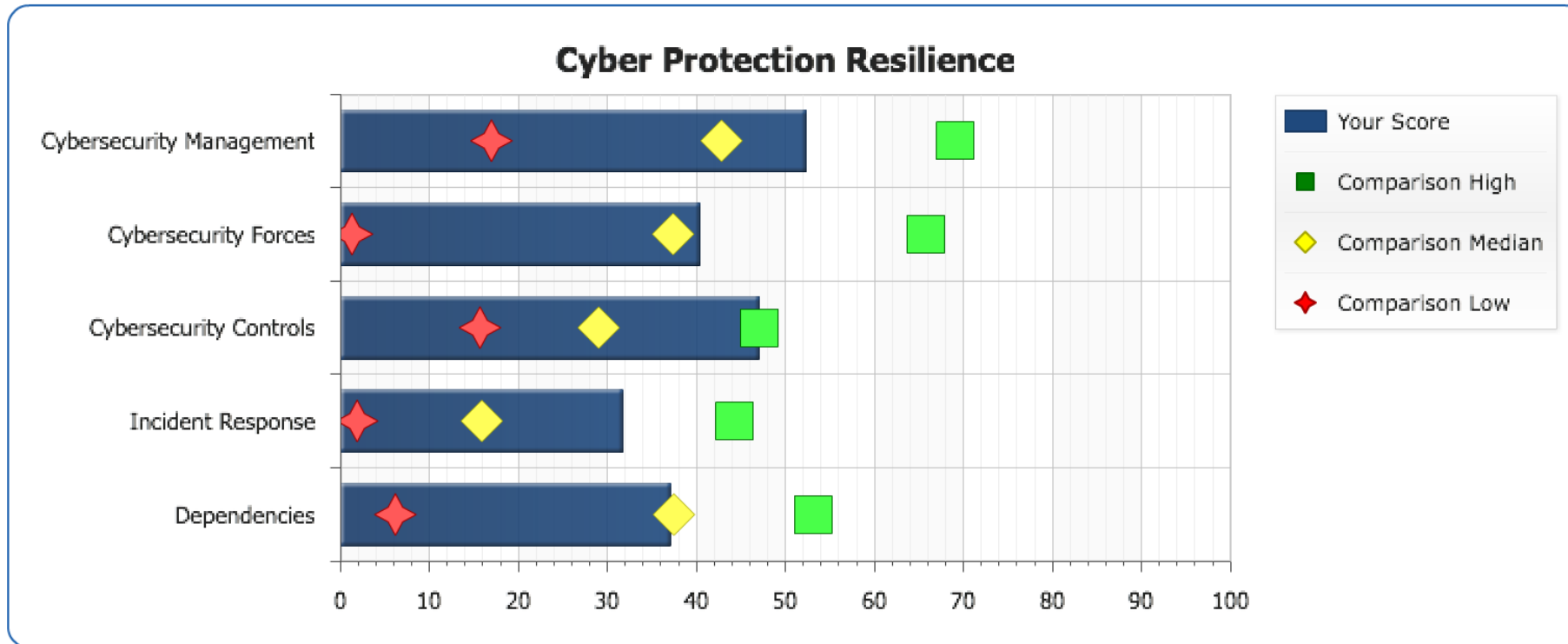
The dashboard displays the following components:

- Header:** CISA Cyber-Infrastructure logo, Home, Logout.
- Left Sidebar:** Cyber Infrastructure Survey for, Cyber Protection Resilience Index, Point Of Contact and Participants, Critical Service Information, Cybersecurity Management, Cybersecurity Leadership, Inventory, System Architecture, Security Architecture, Change Management, Lifecycle Tracking, Accreditation and Assessment, Cybersecurity Plan, Cybersecurity Exercises, External Information Sharing.
- Threat Overlay:** General
- Scenario:** General
- Threat-based PMI:**
 - Natural Disaster
 - Distributed Denial-of-Service
 - Remote Access Compromise
 - System Integrity Compromise
- Scenario:**
 - Where should we to invest?
 - Weakest area in comparison to peers
 - Show management improvement
- Cyber Protection Resilience Chart:**
 - Y-axis: 0 to 100
 - Legend: Your Score (blue square), Comparison High (green square), Comparison Median (yellow diamond), Comparison Low (red diamond)
 - Your Score: ~15
 - Comparison High: ~45
 - Comparison Median: ~35
 - Comparison Low: ~18
- Comparison:**
 - Low Performers
 - Median Performers
 - High Performers



CIS Dashboard - Comparison

- Shows the low, median, and high performers
- Compares your organization to the aggregate

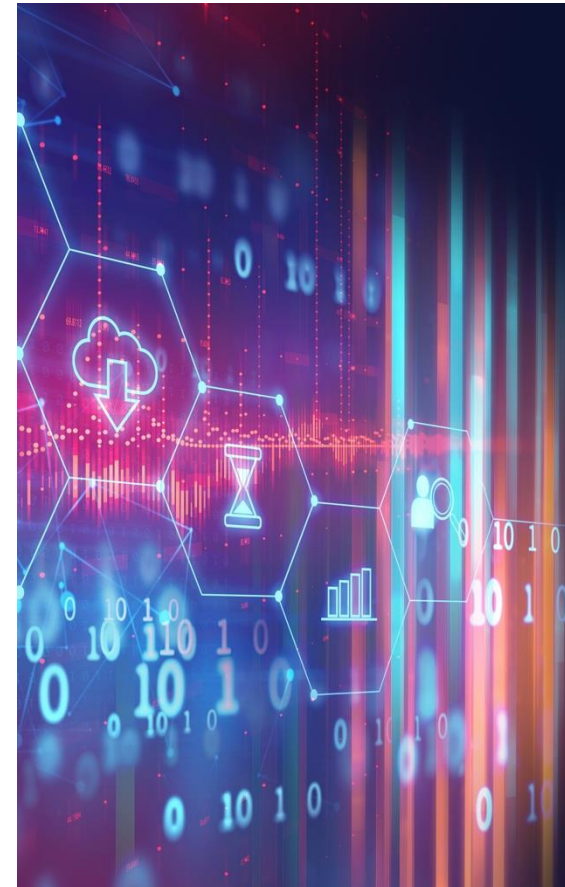


CYBER SECURITY EVALUATION TOOL



Cyber Security Evaluation Tool

- **Purpose:** Assesses control system and information technology network security practices against industry standards.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits:**
 - Immediately available for download upon request
 - Understanding of operational technology and information technology network security practices
 - Ability to drill down on specific areas and issues
 - Helps to integrate cybersecurity into current corporate risk management strategy



PHISHING CAMPAIGN ASSESSMENT



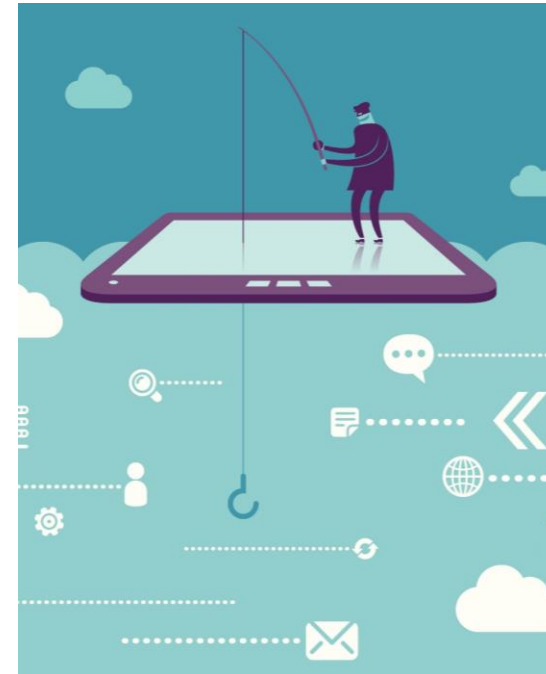
Phishing Campaign Assessment

Purpose: Test an organization's susceptibility and reaction to phishing emails.

Delivery: Online delivery by CISA

Benefits:

- Identify the risk phishing poses to your organization
- Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation
- Receive actionable metrics
- Highlight need for improved security training
- Increase cyber awareness among staff



Phishing Campaign Assessment Sample Email, 1 of 2

To: <Stakeholder List>

From: Apples Customer Relations <freeapplesforyou@[PCA-testing-site].org> Subject: Free iPad – Just Complete a Survey!

Want the new iPad or iPad Mini? I got mine free from this site: <fake link> !!!!!

We would like to invite you to be part of a brand new pilot program to get our new product in the hands of users before official release. This assures that any issues or errors are mitigated before the release. If you are accept to participate in this program all we ask is that you submit a survey at the end of the Pilot. You be able to keep iPad at the end for free!

Apples Customer Relationships Office

Apples Campus, Cupertino, California 95114



Phishing Campaign Assessment Sample Email, 2 of 2

To: <Stakeholder List>
From: OBRM <OBRM@[PCA-testing-site].org>
Subject: Future Budget Plans

In the coming weeks, our state's leadership will be working to draft a plan to prevent long term financial issues and ways to avoid human resource reductions. All departments within the State Government are being directed to draft a plan to help meet projected budget shortages and find ways to reduce spending within the State Government.

We have been asked to work more efficiently with less. As a result, many budgets and programs are also facing significant reduction. The Office of Budget and Resource Management has developed a draft plan that will address any potential budget shortcomings.

To learn more about the budget and how your program maybe affected, please visit <LINK>.

If you have any questions or concerns, we'd love to hear them. Please emails us here <embedded link>.

Office of Budget and Resource Management



CYBER HYGIENE: WEB APPLICATION SCANNING (WAS)



Cyber Hygiene: Web Application Scanning (WAS)

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services. CISA's Cyber Hygiene Web Application Scanning is "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, we can recommend ways to enhance security in accordance with industry and government best practices and standards.



SCANNING OBJECTIVES

- Maintain enterprise awareness of your publicly accessible web-based assets
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities to help reduce overall risk

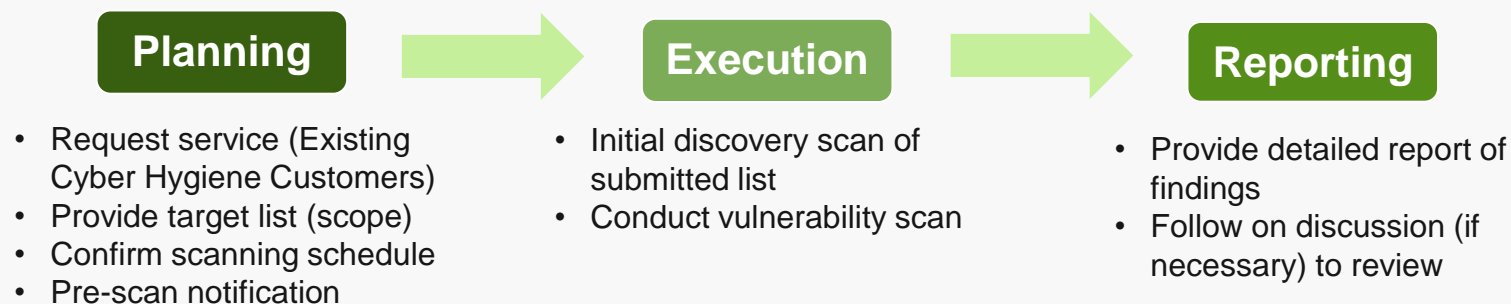


SCANNING PHASES AND OVERALL PROCESS

Scanning Phases

- **Discovery Scanning:** Identify active, internet-facing web applications
- **Vulnerability Scanning:** Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

OVERALL PROCESS



REMOTE PENETRATION TESTING



Remote Penetration Testing

SCENARIOS



External Penetration Test: Verifying if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.



External Web Application Test: Evaluating web applications for potential exploitable vulnerabilities; the test can include automated scanning, manual testing, or a combination of both methods.



Phishing Assessment: Testing the stakeholder email infrastructure through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.



Open-Source Information Gathering: Identify publicly available information about the stakeholder environment which may be useful in preparing for an attack.

ASSESSMENT OBJECTIVES

- Conduct assessments to identify vulnerabilities and work with customers to eliminate exploitable pathways.
- Simulate the tactics and techniques of real-world threats and malicious adversaries.
- Test centralized data repositories and externally accessible assets/resources.
- Avoid causing disruption to the customer's mission, operation, and network infrastructure.

ASSESSMENT TIMELINE

Pre-Planning

- Request RPT
- Receive RPT Capabilities Brief
- Sign and return RPT Rules of Engagement
- Determine RPT services, scope, and logistics during pre-assessment call(s)

Planning

- Confirm schedule
- Establish trusted points of contact

Execution (Up to Six Weeks)

- Dependent on resource availability
- Critical findings are immediately disclosed

Reporting

- Briefing and initial recommendations
- Final report review and receipt – 10 days

Gatewood R4-Georgia-CSA
September 21, 2023



VULNERABILITY SCANNING



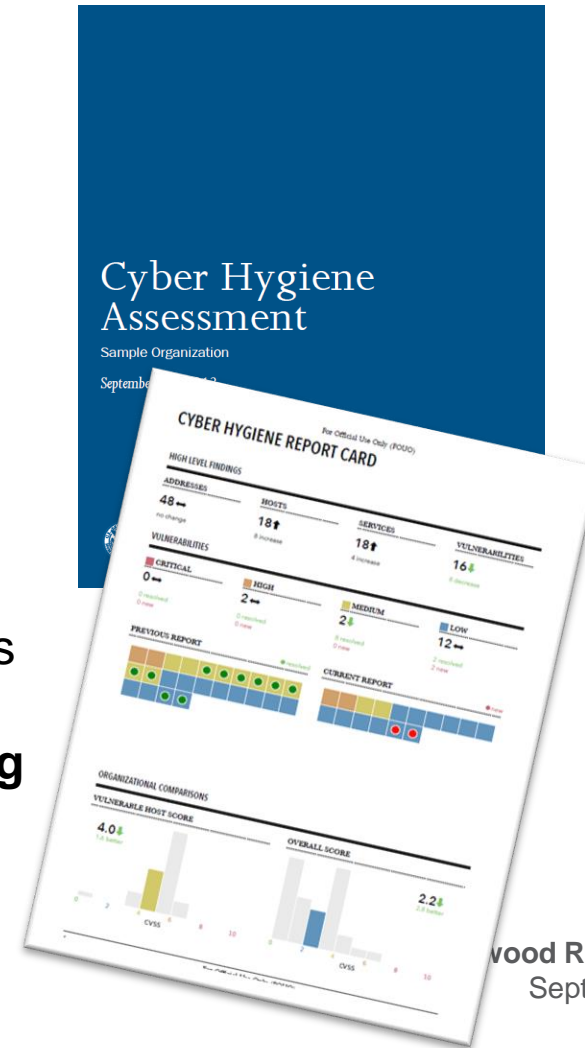
Vulnerability Scanning

Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: Online by CISA

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities
- **Network Vulnerability & Configuration Scanning**
 - Identify network vulnerabilities and weakness



VALIDATED ARCHITECTURE DESIGN REVIEW



Validated Architecture Design Review

Purpose: Analyze network architecture, system configurations, log file review, network traffic and data flows to identify abnormalities in devices and communications traffic.

Delivery: CISA staff working with entity staff

Benefits:

- In-depth review of network and operating system
- Recommendations to improve an organization's operational maturity and enhancing their cybersecurity posture
- Evaluation of network architecture

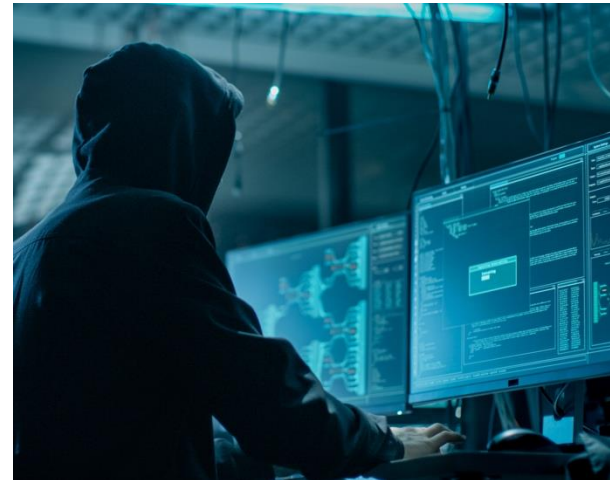


RISK AND VULNERABILITY ASSESSMENT [PENETRATION TEST]



Risk and Vulnerability Assessment

- **Purpose:** Perform network penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks
- **Delivery:** Onsite by CISA
- **Benefits:**
 - Identification of vulnerabilities
 - Specific remediation recommendations
 - Improves an entity's cyber posture, limits exposure, reduces rates of exploitation
 - Increases speed and effectiveness of future cyber attack responses.



Risk and Vulnerability Assessment Specifics

Assessment Aspects

| Service | Description |
|--------------------------------------|--|
| Vulnerability Scanning and Testing | Conduct Vulnerability Assessments |
| Penetration Testing | Exploit weakness, test responses in systems, applications, network, and security controls |
| Social Engineering | Craft e-mail at targeted audience to test security awareness, used as an attack sector to internal network |
| Wireless Discovery & Identification | Identify wireless signals and rogue wireless devices, and exploit access points |
| Web Application Scanning and Testing | Identify web application vulnerabilities |
| Database Scanning | Security Scan of database settings and controls |
| Operating System Scanning | Security Scan of operating system to do compliance checks |



CISA Cyber Assessments in Brief, 1 of 2

| Name | Cyber Resilience Review | Cyber Infrastructure Survey | External Dependencies Management Review | Cybersecurity Evaluation Tool Assessment |
|---------------------------|--|---|--|---|
| Purpose | Identify cybersecurity management capabilities and maturity | Calculate a comparative analysis and valuation of protective measures in-place | Assess the activities and practices utilized by an organization to manage risks arising from external dependencies | Provide detailed, effective, and repeatable methodology for assessing control systems security encompassing the organization's infrastructure, policies, and procedures |
| Scope | Critical service view | Critical service view | Critical service view | Information Technology and Operational Technology systems |
| Time to Execute | 8 Hours (1 business day) | 2 ½ to 4 Hours | 2 ½ to 4 Hours | Varies greatly (min 2 Hours), unknown for self-assessment |
| Information Sought | Capabilities and maturity indicators in 10 security domains | Protective measures in-place | Capabilities and maturity indicators across third-party relationship management lifecycle domains | Architecture diagrams, infrastructure, policies, and procedures documents |
| Preparation | 1-hour questionnaire and planning call(s) | Planning call to scope evaluation | Planning call to scope evaluation | Self-assessment available from web site and used locally |
| Participants | IT / Security Manager, Continuity Planner, and Incident Responders | IT / Security Manager | IT / Security Manager with Continuity Planner and Contract Management | Operators, engineers, IT staff, policy / management personnel, and subject matter experts |
| Delivered By | CSAs iodregionaloperations@cisa.dhs.gov | CSAs iodregionaloperations@cisa.dhs.gov v | CSAs iodregionaloperations@cisa.dhs.gov | Self-administered / CSAs https://ics-cert.us-cert.gov/ |



CISA Cyber Assessments in Brief, 2 of 2

| Name | Validated Architecture Design Review | Phishing Campaign Assessment | Risk and Vulnerability Assessment | Vulnerability Scanning |
|--------------------|--|---|---|---|
| Purpose | Provide analysis and representation of asset owner's network traffic, data flows, and relationships between devices and identifies anomalous communications flows. | Measure the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks. | Perform penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks | Identify public-facing Internet security risks, at a high-level, through service enumeration and vulnerability scanning |
| Scope | Industrial Control Systems / Network Architecture, Traffic | Organization / Business Unit / Email Exchange Service | Organization / Business Unit / Network-Based IT Service | Public-Facing, Network-Based IT Service |
| Time to Execute | Variable (Hours to Days) | Approximately 6 Weeks | Variable (Days to Weeks) | Variable (Hours to Continuous) |
| Information Sought | Network design, configurations, log files, interdependencies, data flows and its applications | Click rate metrics gathered during phishing assessment | Low-level options and recommendations for improving IT network and system security | High-level network service and vulnerability information |
| Preparation | Coordinated via Email. Planning call(s). | Formal rules of engagement and pre-planning | Formal rules of engagement and extensive pre-planning | Formal rules of engagement and extensive pre-planning |
| Participants | Control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs | IT/Security Manager and Network Administrators, end users | IT/Security Manager and Network Administrators | IT/Security Manager and Network Administrators |
| Delivered By | VM VM@CISA.DHS.GOV | VM VM@CISA.DHS.GOV | VM VM@CISA.DHS.GOV | VM VM@CISA.DHS.GOV |



INFORMATION SHARING



AUTOMATED INDICATOR SHARING



Automated Indicator Sharing

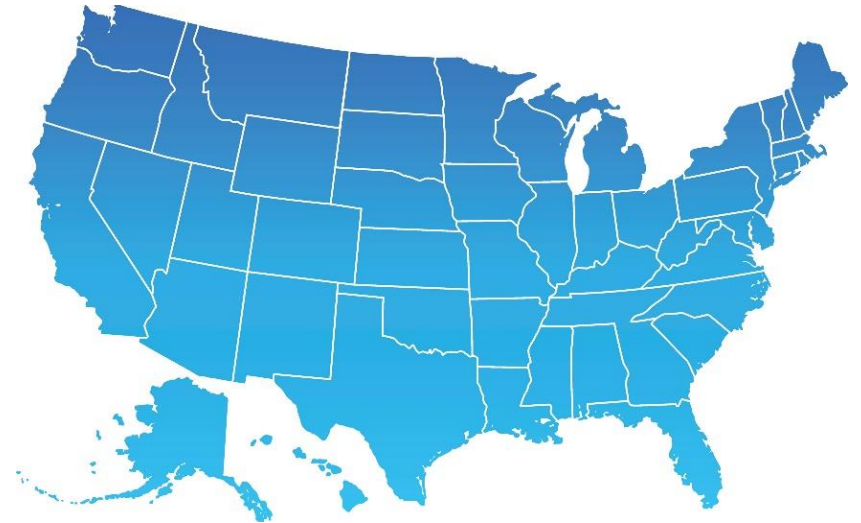
- Automated Indicator Sharing (AIS): Rapid and wide sharing of machine-readable cyber threat indicators and defensive measures at machine-speed for network defense purposes
- AIS is about volume and velocity of sharing indicators, **not** human validation.



Additional Information Sharing Opportunities, 2 of 2

- Multi-State Information Sharing and Analysis Center

- Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
- Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org



- ISACs and ISAOs

- **Information Sharing and Analysis Centers (ISACs)** or **Organizations (ISAOs)** are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.



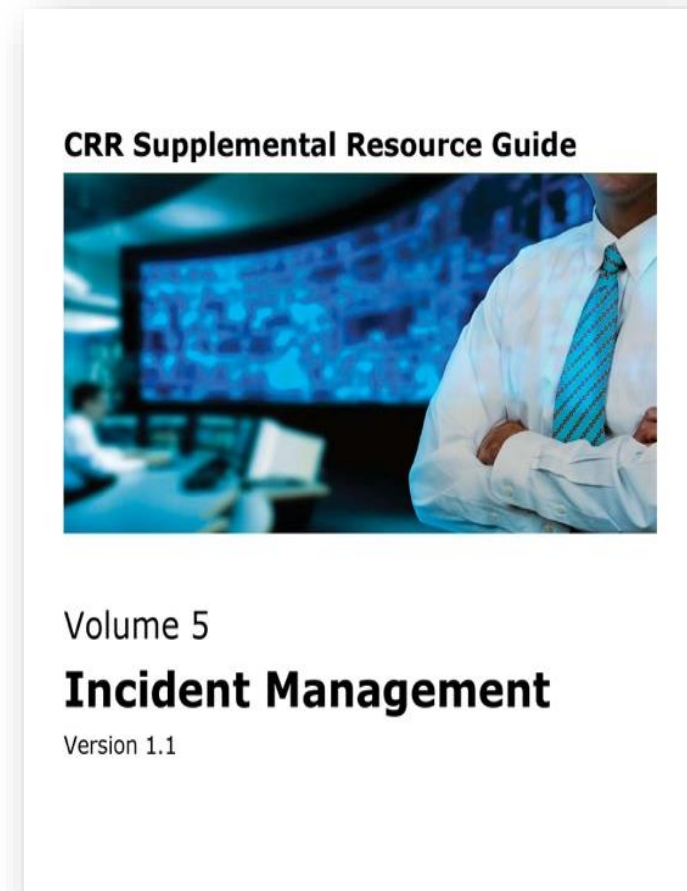
INCIDENT MANAGEMENT



Incident Management Planning Helps Mitigate Effects

1. Get leadership support for incident management planning.
2. Establish an event-detection process.
3. Establish a triage-and-analysis process.
4. Establish an incident-declaration process.
5. Establish an incident-response and recovery process.
6. Establish an incident-communications process.
7. Assign roles and responsibilities for incident management.
8. Establish a post-incident analysis and improvement process.

Resource: CRR Supplemental Resource Guide, Incident Management.



Federal Incident Response, 1 of 2

Federal Incident Response

- **Threat Response:** Attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. Conducting criminal investigations and other actions to counter the malicious cyber activity.
- **Asset Response:** Protecting assets and mitigating vulnerabilities in the face of malicious cyber activity, reducing the impact to systems and data; strengthening, recovering, and restoring services; identifying other entities at risk; and assessing potential risk to broader community.



Federal Incident Response, 2 of 2

Threat Response

Federal Bureau of Investigation

855-292-3937 or cywatch@ic.fbi.gov

U.S. Secret Service

secretservice.gov/contact/field-offices

Immigration and Customs

Homeland Security Investigations

866-347-2423 or ice.gov/contact/hsi

Asset Response

CISA Central

888-282-0870 or central@cisa.DHS.gov

Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

Report Internet Crimes:

FBI Internet Crime Complaint Center

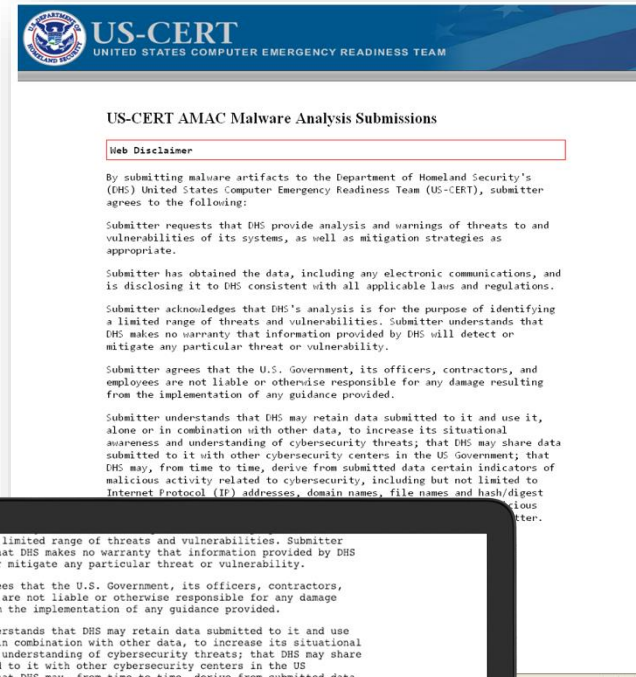
ic3.gov



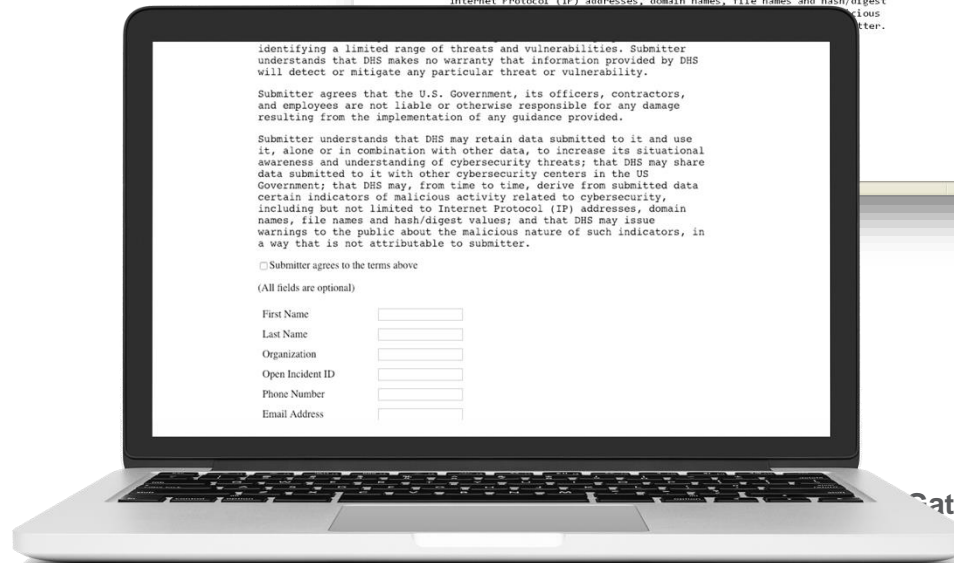
Malware Analysis

To submit malware:

- Email submissions to CISA Central at: submit@malware.us-cert.gov
 - Send in password-protected zip file(s). Use password “infected.”
- Upload submission online: <https://malware.us-cert.gov>



The screenshot shows the top portion of a web form titled "US-CERT AMAC Malware Analysis Submissions". At the top left is the US-CERT logo with the text "UNITED STATES COMPUTER EMERGENCY READINESS TEAM". Below the title is a "Web Disclaimer" section with a red border. The text of the disclaimer includes: "By submitting malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), submitter agrees to the following: Submitter requests that DHS provide analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate. Submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations. Submitter acknowledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability. Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided. Submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the US Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values; and that DHS may issue warnings to the public about the malicious nature of such indicators, in a way that is not attributable to submitter."



The screenshot shows the bottom portion of the form on a laptop screen. It includes the text: "identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability. Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided. Submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the US Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values; and that DHS may issue warnings to the public about the malicious nature of such indicators, in a way that is not attributable to submitter." Below this text is a checkbox labeled "Submitter agrees to the terms above" and the text "(All fields are optional)". There are six input fields: "First Name", "Last Name", "Organization", "Open Incident ID", "Phone Number", and "Email Address", each with a corresponding empty text box.



ADDITIONAL CYBERSECURITY RESOURCES



Cyber Exercises and Planning

CISA's National Cyber Exercise and Planning Program develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

- Cyber Storm Exercise – DHS's flagship national-level biennial exercise
- Exercise Planning and Conduct
- Cyber Exercise Consulting and Subject Expertise Support
- Cyber Planning Support
- Off-the-Shelf Resources



Gatewood R4-Georgia-CSA
September 21, 2023

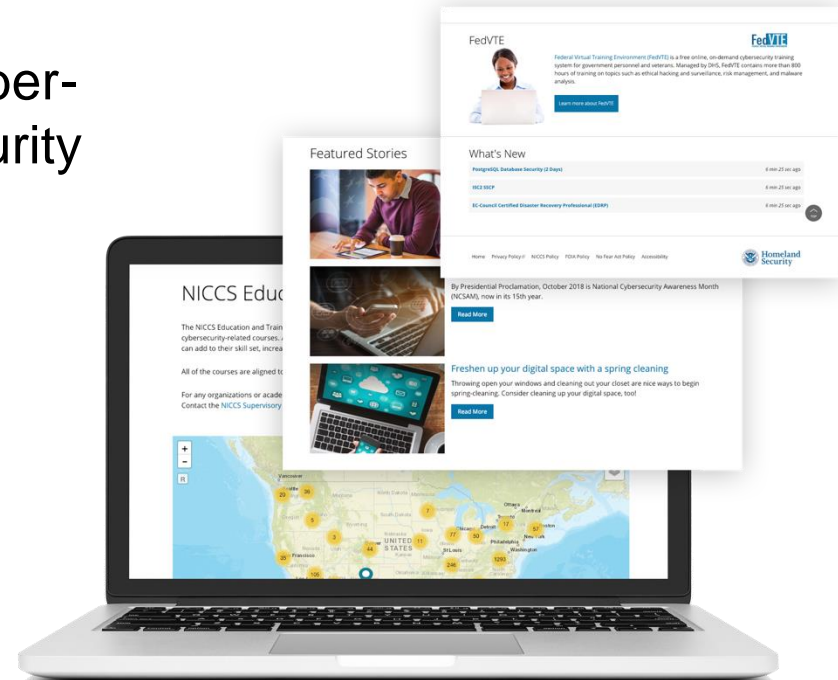


Cybersecurity Training Resources

CISA offers easily accessible education and awareness resources through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Searchable Training Catalog with 4,400 plus cyber-related courses offered by nationwide cybersecurity educators
- Interactive National Cybersecurity Workforce Framework
- Cybersecurity Program information: FedVTE, Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
- Tools and resources for cyber managers
- Upcoming cybersecurity events list



For more information, visit NICC.US-CERT.gov

Our Nation's Cyber Workforce Foundation

The **National Cybersecurity Workforce Framework** is a collection of definitions that describe types of cybersecurity work and skills requires to perform it.

- ✓ When used nationally, the definitions help establish universally applicable cybersecurity skills, training/development, and curricula
- ✓ 7 Categories, 30+ Specialty Areas
- ✓ Baselines knowledge, skills, and abilities & tasks



Operate & Maintain



Securely Provision



Analyze



Collect & Operate



Oversight & Development



Protect & Defend



Investigate



Free Federal Cyber Training

FedVTE enables cyber professionals to continue growing skills.

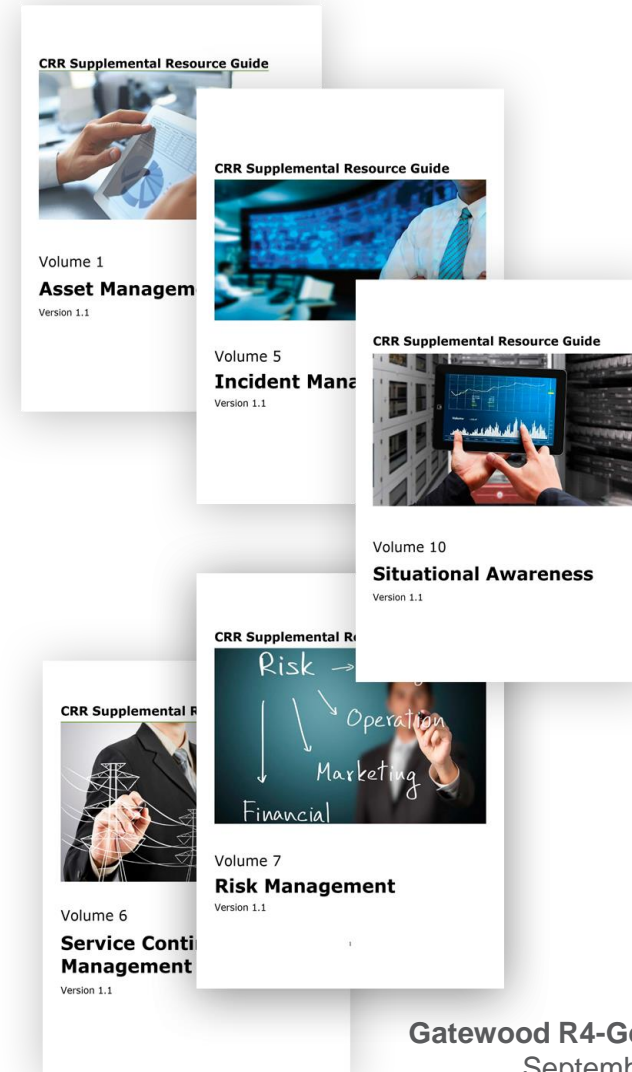
FedVTE is an online, on-demand training center that provides **free** cybersecurity training for U.S. veterans and federal, state, local, tribal, and territorial government employees. **As of January 2017**, there are:

- Over 140,000 registered users, including employees at all levels of government
- Over 18,000 veteran users (through non-profit partner, Hire Our Heroes™)
- Over 5,000 SLTT registered users



Resource Guides

- **Resource Guides:** Created to help organizations enhance their resilience in specific Cyber Resilience Review (CRR) domains.
- **CRR Tools:** Helps move organizations from initial capability to well-define capability in security management areas
- **CRR Domains:** Includes the CRR 10 “domains” each representing a capability area foundational to an organization’s cyber resilience.
- **Content:** While the guides were developed for organizations to utilize after conducting a CRR, these publications provide content useful for all organizations with cybersecurity equities.
- **Flexibility in Use:** Moreover, the guides can be utilized as a full set or as individual components, depending on organizational preference and/or need.
- For more information, visit <https://www.cisa.gov/cyber-resource-hub>



Contact



General Inquiries

iodregionaloperations@cisa.dhs.gov

CISA Contact Information

Name
Title

@cisa.dhs.gov
Number

Number

@cisa.dhs.gov
+1 202-380-6024

Cybersecurity and Infrastructure Security Agency



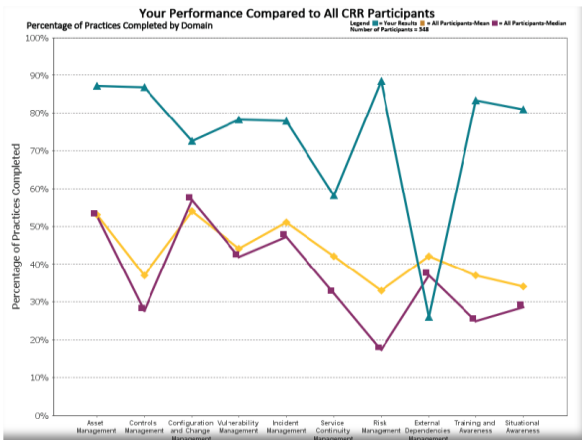
BACK-UP SLIDES



CRR Sample Report



Each CRR report includes:



Comparison data with other CRR participants
*facilitated only



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

| ML-1 | ML-2 | ML-3 | ML-4 | ML-5 |
|------|------|------|------|------|
| GI | G2 | G3 | G4 | G5 |
| G6 | G7 | TI1 | TI2 | TI3 |
| TI4 | TI5 | TI6 | TI7 | TI8 |

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.

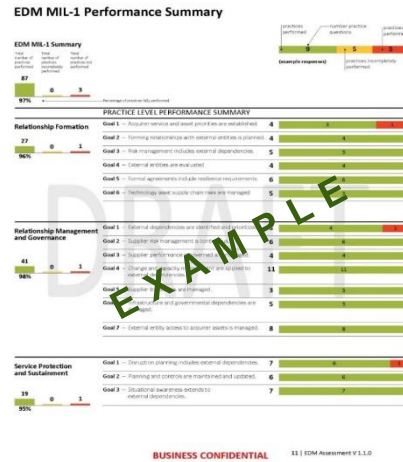
| Goal 1 – Identify & prioritize critical services | | | | | | | | | |
|---|---|--------|------------|-------------|------------|------------|------------|------------|-----|
| 1. Are critical services identified? [SC.SG2.SP1] | Yes | | | | | | | | |
| 2. Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC.SG2.SP1] | Incomplete | | | | | | | | |
| Q2 CERT-RMM Reference: [SC.SG2.SP1] Identify and prioritize 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] | <table border="1"> <tr><td>People</td><td>Incomplete</td></tr> <tr><td>Information</td><td>Incomplete</td></tr> <tr><td>Technology</td><td>Incomplete</td></tr> <tr><td>Facilities</td><td>Yes</td></tr> </table> | People | Incomplete | Information | Incomplete | Technology | Incomplete | Facilities | Yes |
| People | Incomplete | | | | | | | | |
| Information | Incomplete | | | | | | | | |
| Technology | Incomplete | | | | | | | | |
| Facilities | Yes | | | | | | | | |
| 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) | | | | | | | | | |



EDM Assessment Report

Each EDM report includes:

- Performance summary of existing capability managing external dependencies



- Sub-domain performance of existing capability managing external dependencies and options for consideration for all responses

Relationship Formation

1 Relationship Formation

| Goal 1 | Goal 2 | Goal 3 | Goal 4 | Goal 5 | Goal 6 |
|--------|--------|--------|--------|--------|--------|
| ■ | ■ | ■ | ■ | ■ | ■ |

The purpose of relationship formation is to assess whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them. Relationship formation includes understanding the acquirer's critical services, having a process for entering into formal relationships, and evaluating external entities. A key aspect of relationship formation is identifying resilience requirements as the basis for risk management and formal agreements. Resilience requirements typically focus on integrity, confidentiality, and availability, but can also include other requirements important to the critical service.

Goal 1 - Acquirer service and asset priorities are established.

The purpose of this goal is to assess whether the acquirer has identified its own critical services, assets, and control objectives because these are fundamental activities for effectively managing external dependencies.

| | |
|---|-----|
| 1. Are the acquirer's services identified and documented across the enterprise? (SC-SG2.SP1) | Yes |
| 2. Are the acquirer's services prioritized based on an analysis of the operational impact of services are disrupted? (SC-SG2.SP1) | No |
| 3. Are the acquirer's assets that directly support the critical services? (SC-SG2.SP1) | Yes |
| 4. Have control objectives been established for the critical services that support the critical services? (CTRL-SG1.SP1) | Yes |

Options for Consideration

01: CSST-SMMS Reference (SC-SG2.SP1) Ignoring acquirer's high-value services

A fundamental risk management principle is to focus on activities to protect and sustain services that most directly affect the acquirer's ability to achieve its mission. This practice recommends identifying the assessed acquirer's high-value services, which it provides to its customers and other stakeholders.

NIST Reference:
 NIST Special Publication 800-53 Revision 4, "Recommended Security Controls for Federal Information Systems and Organizations": The Fundamentals, 2.1 Multitiered Risk Management.

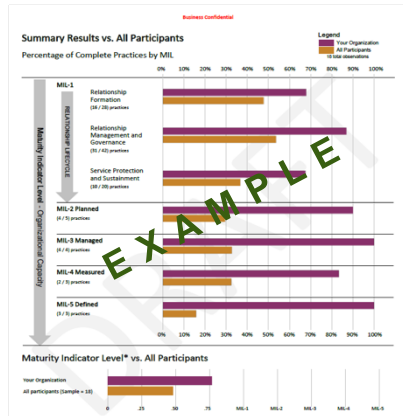
To integrate the risk management process throughout the organization and more effectively address mission/business concerns, a tiered approach is employed that addresses risk at the (i) organizational level; (ii) mission/business process level; and (iii) information system level.

Tier 1 provides a prioritization of organizational missions/business functions which in turn drives investment strategies and funding decisions -promoting cost-effective, efficient information technology solutions consistent with the strategic goals and objectives of the organization and measures of performance.

NIST CSF Version 2.0, (ID.AM, Section 3.2 Establishing or Improving a Cybersecurity Program, Step 1.

14 | EDM Assessment V 1.1.0

- Comparison data with other EDM participants





Stanton Gatewood

DHS/CISA

Cyber Security Coordinator/Advisor,
Region 4 - Georgia

Email: stanton.gatewood@cisa.dhs.gov

