Cyber Security Assessments

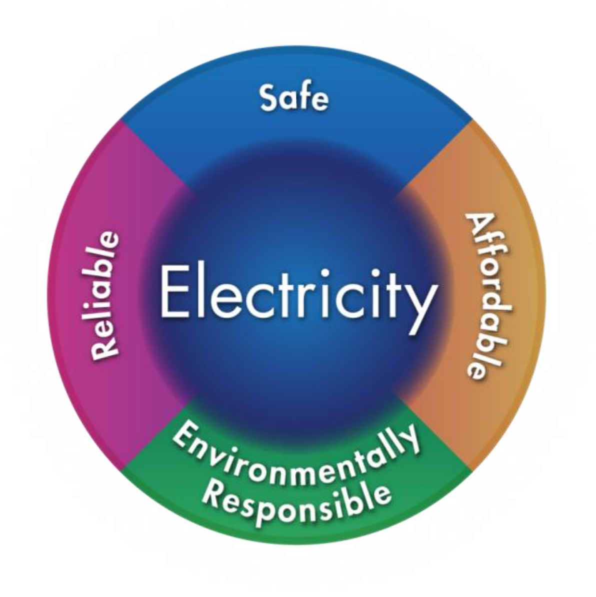
USAID-USEA Digitalization and Cyber Security Webinar Series

Galen Rasche
Senior Program Manager, EPRI
grasche@epri.com

September 3, 2020

About EPRI (www.epri.com)

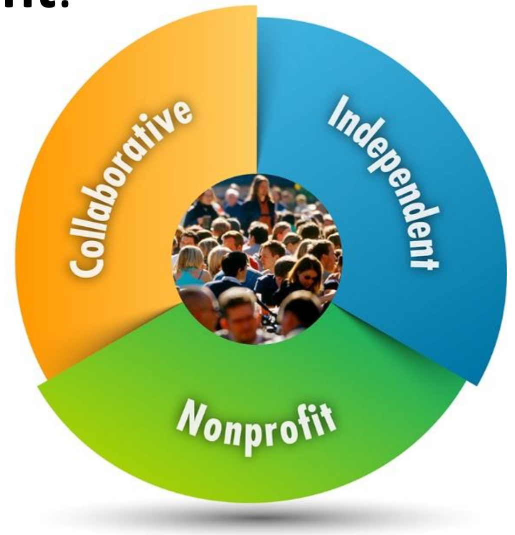
ELECTRIC POWER RESEARCH INSTITUTE



- EPRI conducts **research and development** relating to the **generation**, **delivery** and **use of electricity** for the benefit of the public.

- EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including **reliability**, **efficiency**, **affordability**, **health**, **safety** and the **environment**.

- **EPRI members** represent 90% of the electricity generated and delivered in the United States with international participation extending to nearly **40 countries**.

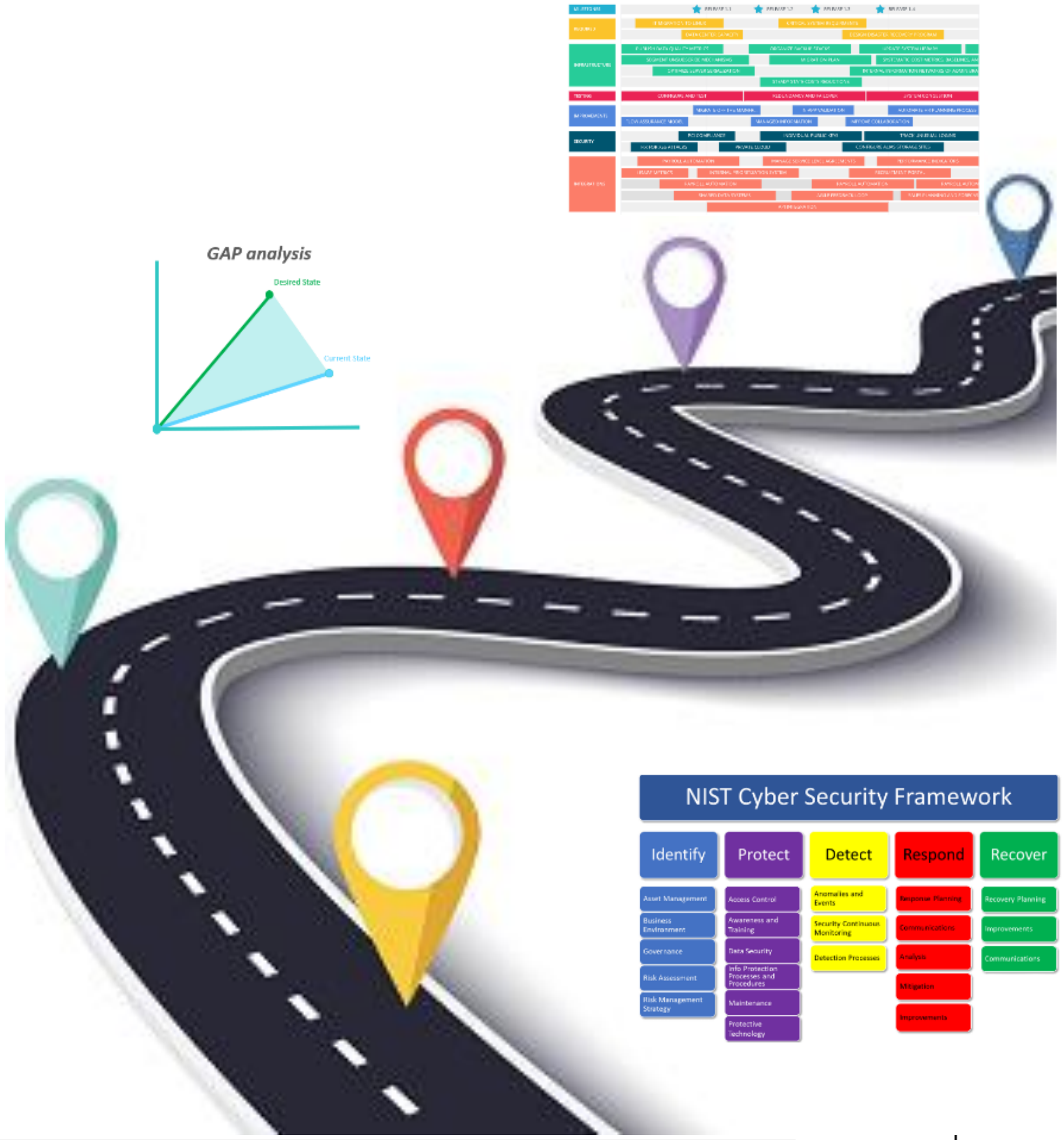


Social Media: Facebook | LinkedIn | Twitter | YouTube

Cyber Security Assessments for Electric Power Utilities

Cyber Security Assessments

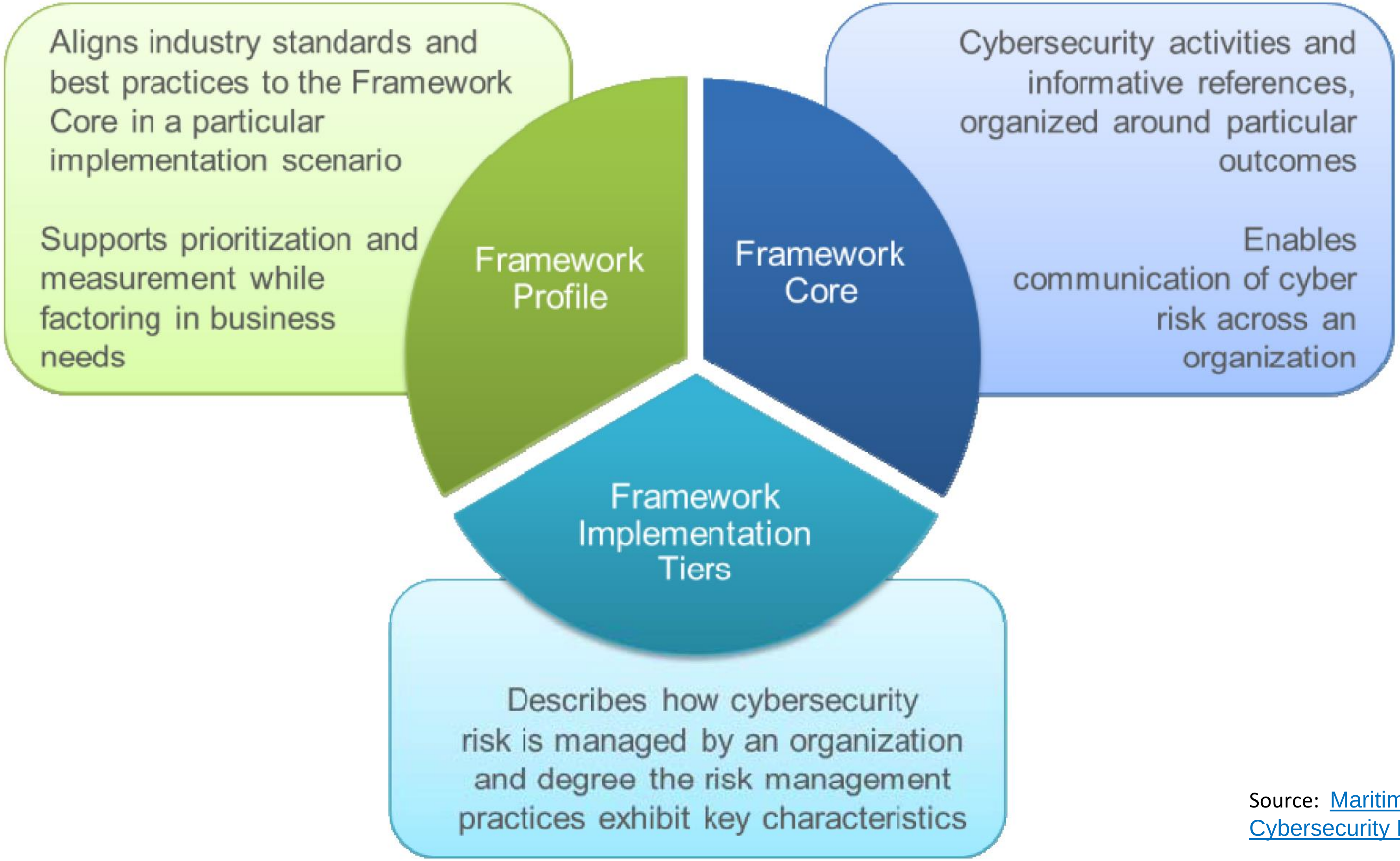
- *Where are we now?*
    - *Current state assessment*
- *Where do we want to be?*
    - *Desired future state*
- *How do we get there?*
    - *Identify required capabilities to achieve future state*
    - *Develop Cybersecurity Program Roadmap and implementation plans*



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Elements of the NIST Cybersecurity Framework (CSF)



Framework Profile

Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

Supports prioritization and measurement while factoring in business needs

Framework Core

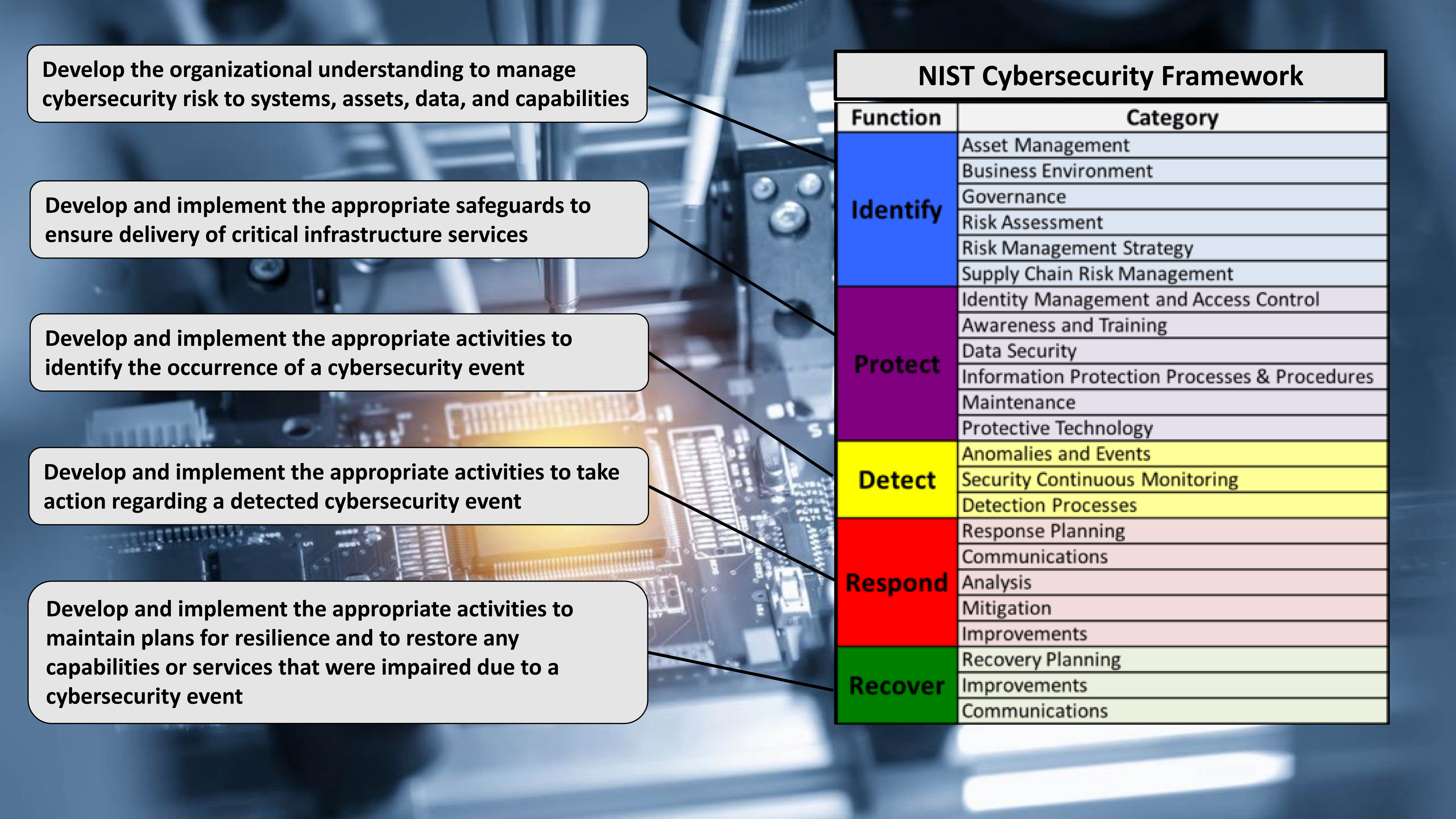
Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Framework Implementation Tiers

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Source: Maritime Bulk Liquids Transfer Cybersecurity Framework Profile



Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services

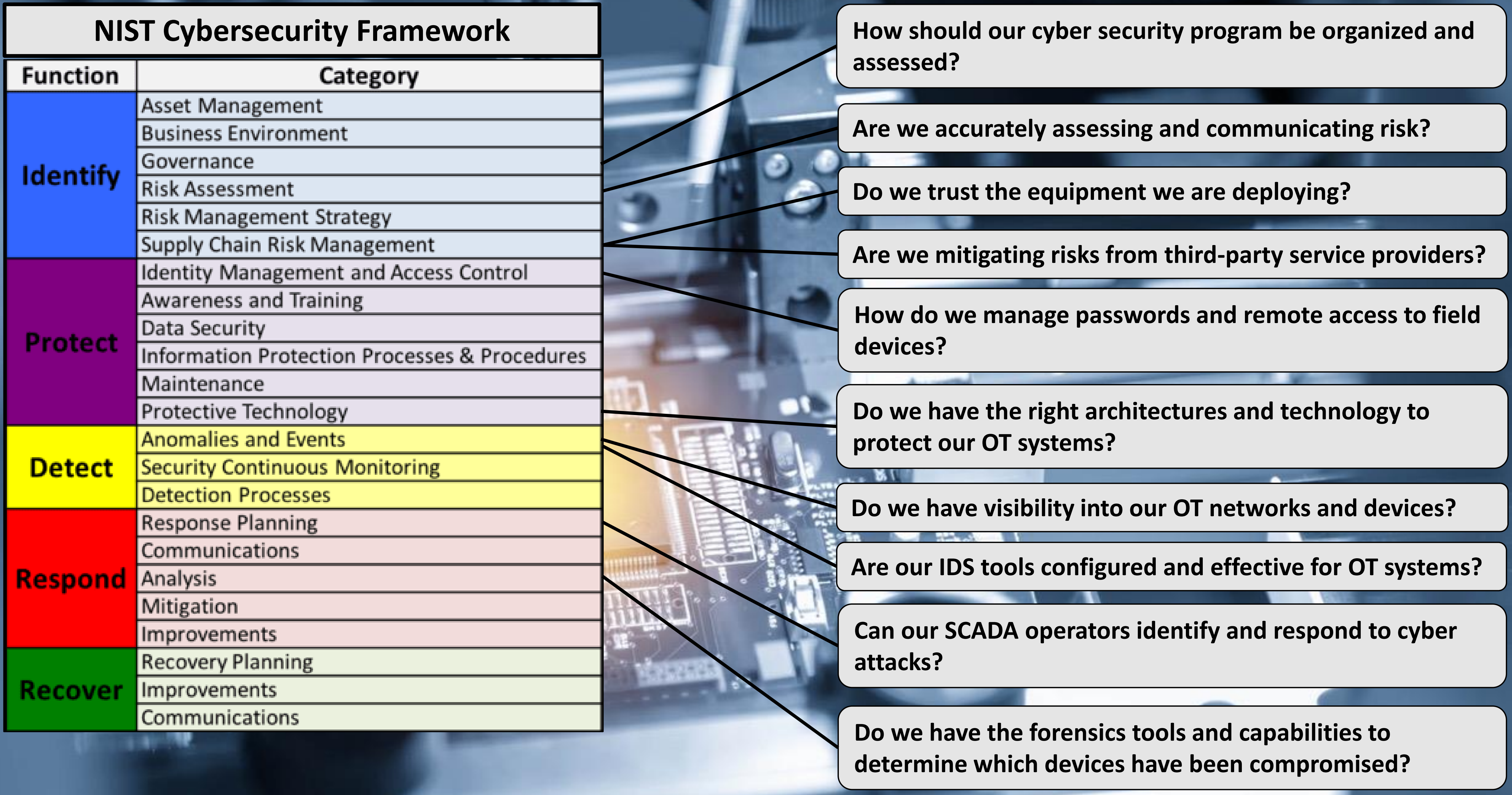
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

NIST Cybersecurity Framework

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications



NIST Cybersecurity Framework

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

How should our cyber security program be organized and assessed?

Are we accurately assessing and communicating risk?

Do we trust the equipment we are deploying?

Are we mitigating risks from third-party service providers?

How do we manage passwords and remote access to field devices?

Do we have the right architectures and technology to protect our OT systems?

Do we have visibility into our OT networks and devices?

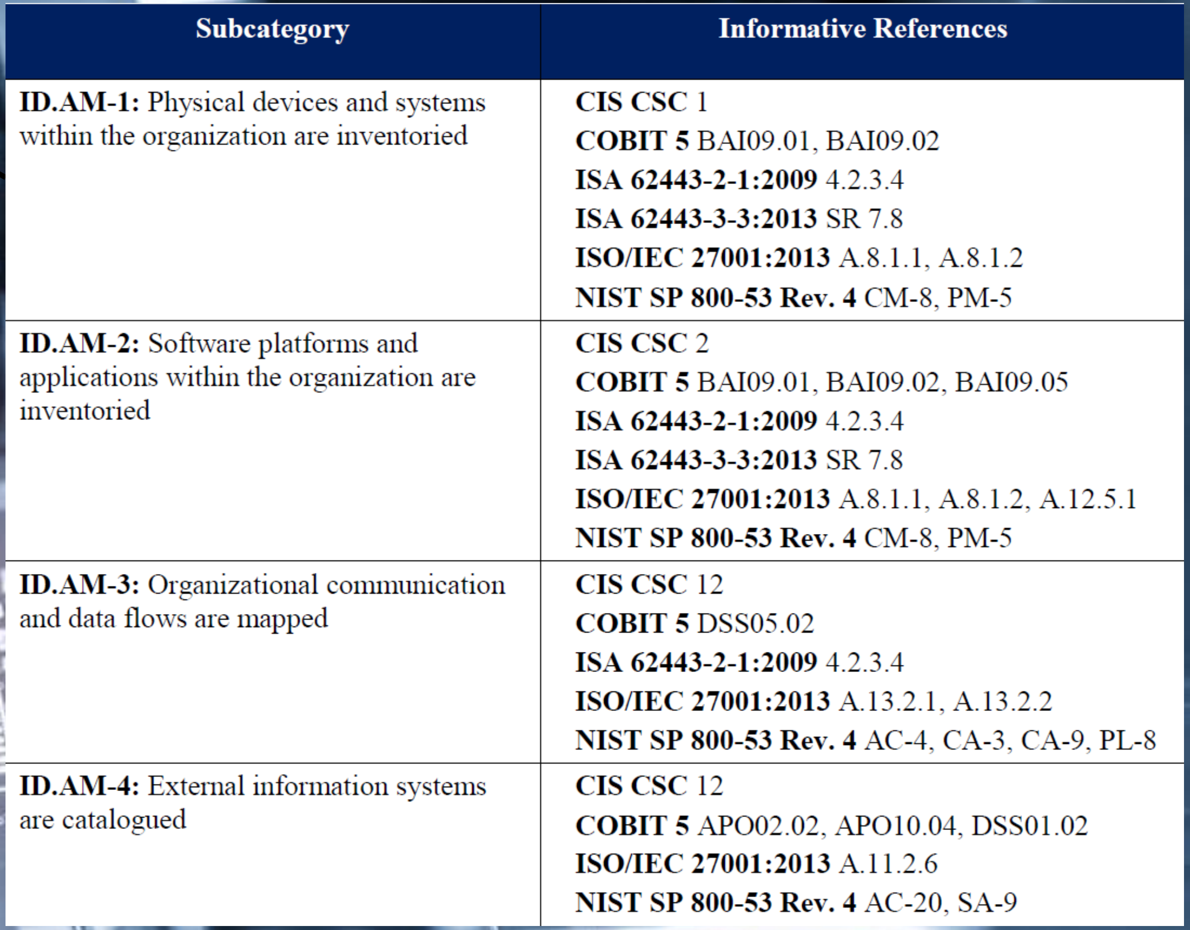
Are our IDS tools configured and effective for OT systems?

Can our SCADA operators identify and respond to cyber attacks?

Do we have the forensics tools and capabilities to determine which devices have been compromised?

NIST Cybersecurity Framework

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications



Subcategory	Informative References
ID.AM-1: Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9

Benefits

- Five functions easy for non-security staff and executives to understand
- Widely adopted in the industry
- Focuses on ***outcomes*** – flexible implementation
- Industry profiles and implementation guides available
- Can be implemented with various international cyber security standards and controls catalogues

Challenges

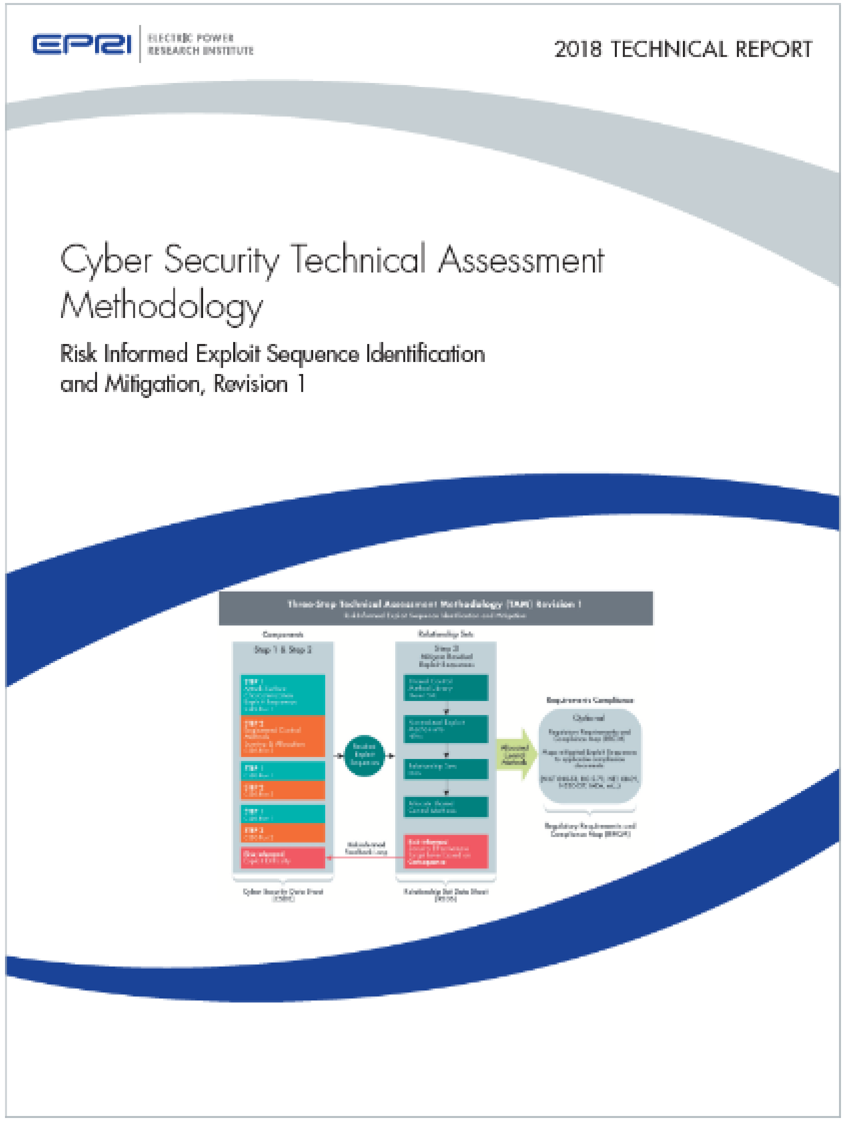
- No generally accepted scoring mechanism
- Control set is at different levels
- Different tiers are not a formal maturity model
- Need OT cyber security expertise to correctly apply the Framework to electric power utility operations domains

NIST Cybersecurity Framework Resources

- NIST Cybersecurity Framework (CSF) Version 1.1
- NIST TN 2051 – Cybersecurity Framework Smart Grid Profile
- Maritime Bulk Liquids Transfer Cybersecurity Framework Profile
- NIST IR 8183 - Cybersecurity Framework Manufacturing Profile
- NIST IR 8183A - Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide

EPRI Technical Assessment Methodology

Technical Assessment Methodology (TAM) Purpose



2018 TECHNICAL REPORT

Cyber Security Technical Assessment Methodology

Risk Informed Exploit Sequence Identification and Mitigation, Revision 1

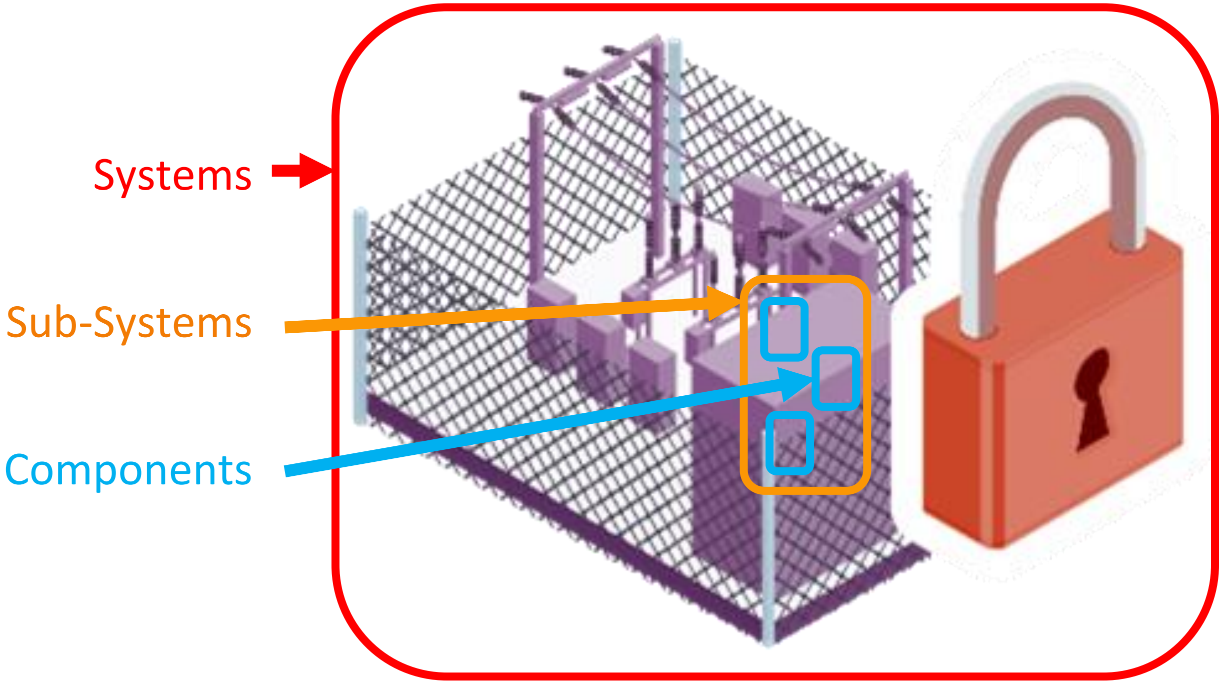
Three-Step Technical Assessment Methodology (TAM) Revision 1
Risk Informed Exploit Sequence Identification and Mitigation
Components
Step 1 & Step 2
Relationship Sets
Step 3
Requirements Compliance
Optional
Cyber Security Data Sheet (CSDS)
Relationship Set Data Sheet (RSDS)
Regulatory Requirements and Compliance Map (RRCM)

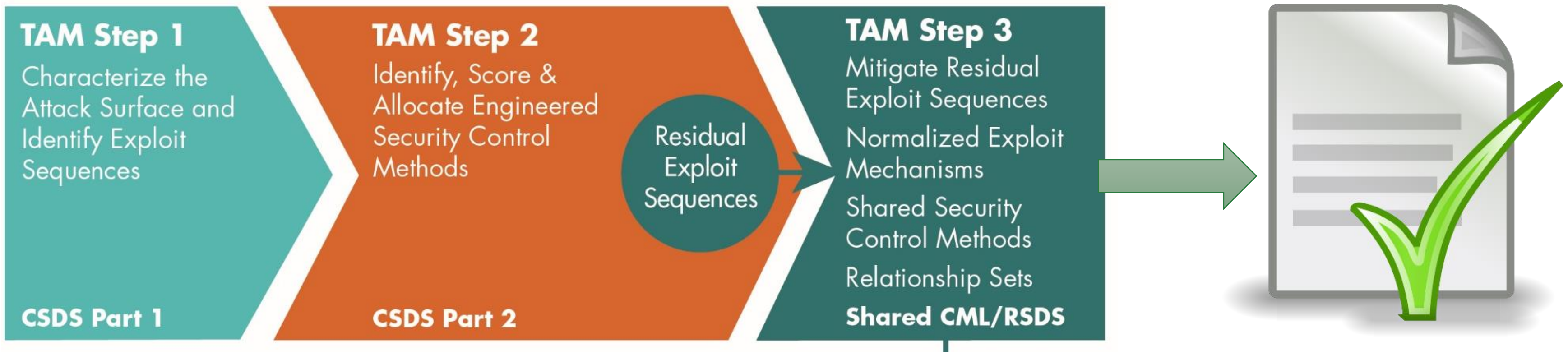
Provides an actionable, risk-informed, systems engineered based approach that guides users to:

- Understand their systems and components,
- Analyze the actual vulnerabilities and how the system can be attacked,
- Mitigate those vulnerabilities to an acceptable risk level,
- By applying effective control measures.

The EPRI Technical Assessment Methodology (TAM)

- Security Risk Assessment of Systems, Sub-Systems or Components
- Scoring risks of existing control measures (effectiveness and burden)
- For Procurement or Installed Equipment
- Determines Mitigations & Unmitigated Vulnerabilities
- Identifies parties responsible for Mitigations





TAM Step 1

Characterize the Attack Surface and Identify Exploit Sequences

CSDS Part 1

TAM Step 2

Identify, Score & Allocate Engineered Security Control Methods

CSDS Part 2

Residual Exploit Sequences

TAM Step 3

Mitigate Residual Exploit Sequences

Normalized Exploit Mechanisms

Shared Security Control Methods

Relationship Sets

Shared CML/RSDS

Cyber Security Data Sheet (CSDS)

Cyber Security Data Sheet (CSDS)

CSDS Part 1: Attack Surface Characterization

- Part 1a: Assessment Scope
- Part 1b: Target Asset Characteristics
- Part 1c: Attack Pathways
- Part 1d: Exploit Sequences

CSDS Part 2: Identify, Score, & Allocate Control Methods

- Part 2a: Security Control Method Identification and Scoring
- Part 2b: Allocation of Security Control Methods

Output of the Process

Cyber Security Data Sheets (CSDS)

- Identify attack surface
- Scoring of existing control measures (effectiveness and burden)
- Unmitigated vulnerabilities
- What if analysis of additional control measures
- Standardized and scalable

Relationships Sets

- Systems and component communication
- Data flows
- Shared control measures
- Aids in incident response

Library of administrative and shared technical control methods

Technical Assessment Methodology Resources

- Cyber Security Technical Assessment Methodology, Risk Informed Exploit Sequence Identification and Mitigation, Revision 1
- EPRI Cyber Security Technical Assessment Methodology Video (3.43 min)
- Toward a New Risk-Informed Approach to Cyber Security
- SEL 487E Protective Relay Reference Cyber Security Data Sheet (CSDS): Cyber Security Technical Assessment Methodology Use Case Study (3002017149)
- Domain Controller Cyber Security Data Sheet (CSDS) Topical Guide (3002015759)
- Risk Informed Target Level Topical Guide (3002015760)
- Cyber Security Data Flow Identification and Documentation Topical Guide (3002015761)

Contact:

Galen Rasche
Sr. Program Manager
grasche@epri.com

Together…Shaping the Future of Electricity