ISA New Orleans Section

February 2018 Section Meeting

Welcome Aboard

ISA New Orleans Section

Say Hello to our New Sponsor

Section Sponsor

$150 Annually

Benefits:

- Logo, company information, and your company's website link displayed on the ISA New Orleans Section website.
- Logo on signage present at all section meetings and events.
- Priority opportunity to present technical topics at ISA New Orleans Section meetings and events.
- Priority opportunity to sponsor section meetings and events.
- Opportunity to be a Table-Top exhibitor at sponsored section meetings and events.
- Your company listed in our Local Directory of Automation Suppliers.

Thank You to All of Our Sponsors!

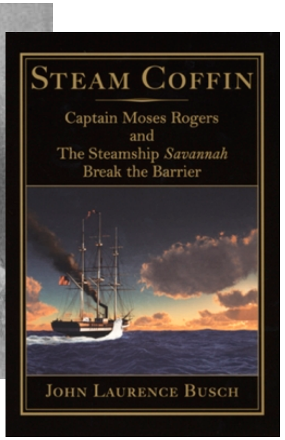
LATTER & BLUM
Since 1916 INC/REALTORS
Serving the Gulf South for 100 years - and just getting started!

Barbara J. Brock, ABR
504-362-1823 • 504-655-0523
www.barbaraj.brock.latter-blum.com

MSB
M S Benbow and Associates
A Professional Engineering Corporation
www.msbenbow.com

Upcoming Section Meetings

March 13th
Building the First "Steamship" in History



Steam Coffin

Captain Moses Rogers
and
The Steamship *Savannah*
Break the Barrier

John Laurence Busch

THE UNIVERSITY *of*
NEW ORLEANS

Future Dates:

- April 10th
- May 8th
- June 5th
- July 10th
- August 7th

Topics/Speakers in Development:

- Ethics with LAPELS – *April or May*
- Nick Sands – *June*
- Paul Gruhn – *tbd*
- Champion Technologies – *tbd*
- Petrotech – *tbd*
- Process Solutions - *tbd*

Other Upcoming ISA Activities

- **District 7 Leadership Meeting**
  - April 20-21
  - Galveston, TX
  - Topics on Agenda
    - How to bring new leadership in the local sections
    - Sponsorship best practices – to be presented by Dean Bickerton
    - Using technology such as web-based meetings

Cybersecurity and ISA

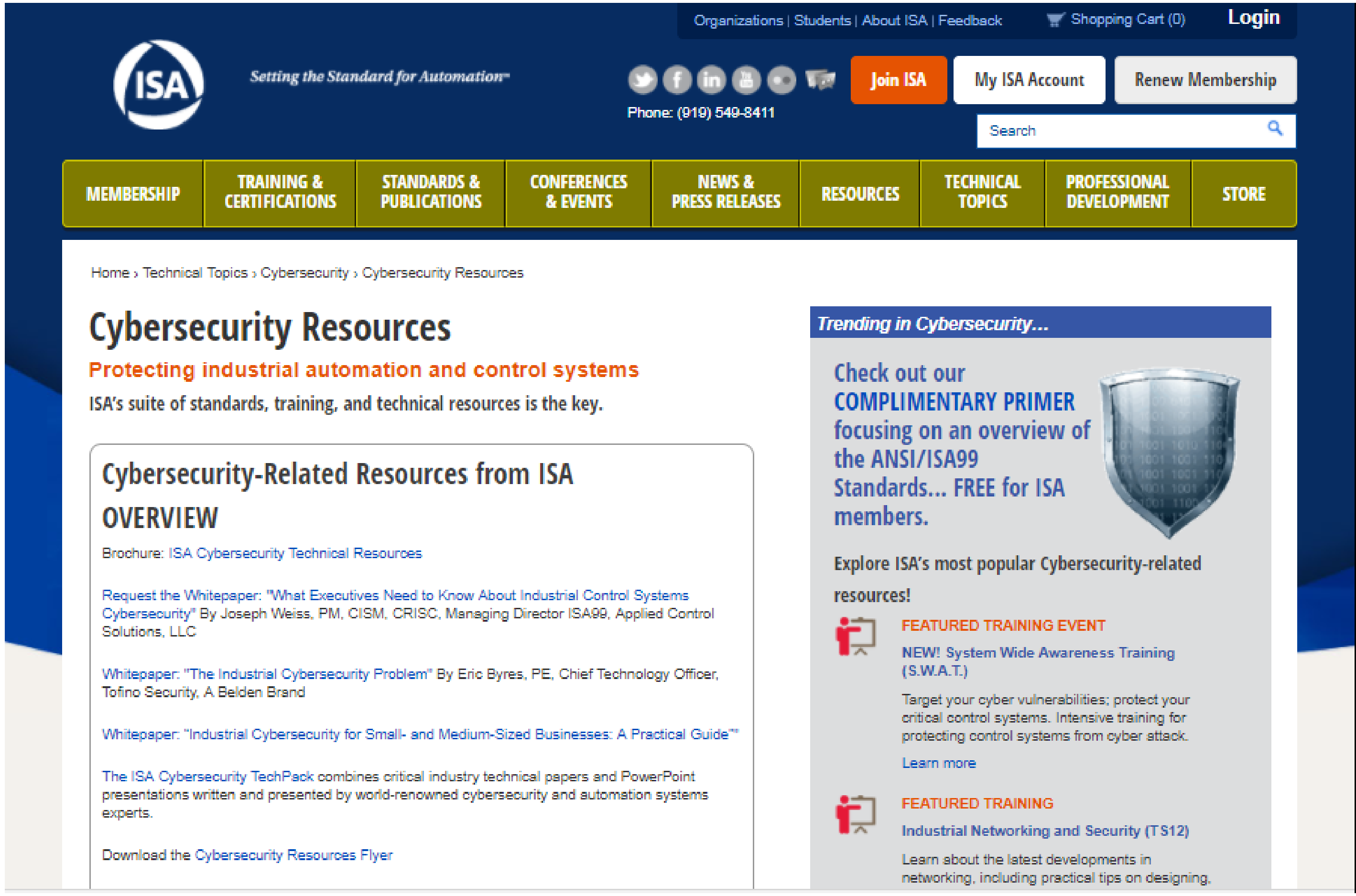
ISA is the developer and applications-focused thought leader behind the world’s only consensus-based industrial cybersecurity standard.

ISA’s approach to the cybersecurity challenge is holistic, bridging the gap between operations and information technology; and between process safety and cybersecurity.

Cybersecurity Resources

ISA New Orleans Section

- **ISA Cybersecurity Resources**
  - Standards
  - Training
  - Certification Programs
  - Whitepapers
  - Conformity Assessment



Home › Technical Topics › Cybersecurity › Cybersecurity Resources

Cybersecurity Resources

Protecting industrial automation and control systems

ISA's suite of standards, training, and technical resources is the key.

Cybersecurity-Related Resources from ISA

OVERVIEW

Brochure: ISA Cybersecurity Technical Resources

Request the Whitepaper: "What Executives Need to Know About Industrial Control Systems Cybersecurity" By Joseph Weiss, PM, CISM, CRISC, Managing Director ISA99, Applied Control Solutions, LLC

Whitepaper: "The Industrial Cybersecurity Problem" By Eric Byres, PE, Chief Technology Officer, Tofino Security, A Belden Brand

Whitepaper: "Industrial Cybersecurity for Small- and Medium-Sized Businesses: A Practical Guide"

The ISA Cybersecurity TechPack combines critical industry technical papers and PowerPoint presentations written and presented by world-renowned cybersecurity and automation systems experts.

Download the Cybersecurity Resources Flyer

Trending in Cybersecurity...

Check out our COMPLIMENTARY PRIMER focusing on an overview of the ANSI/ISA99 Standards... FREE for ISA members.

Explore ISA's most popular Cybersecurity-related resources!

FEATURED TRAINING EVENT

NEW! System Wide Awareness Training (S.W.A.T.)

Target your cyber vulnerabilities; protect your critical control systems. Intensive training for protecting control systems from cyber attack.

Learn more

FEATURED TRAINING

Industrial Networking and Security (TS12)

Learn about the latest developments in networking, including practical tips on designing.

isa.org – Technical Topics – Cybersecurity

Executive Order 13636

Signed February 12, 2013

Executive Order 13636 outlines responsibilities for Federal Departments and Agencies to aid in Improving **Critical Infrastructure** Cybersecurity.

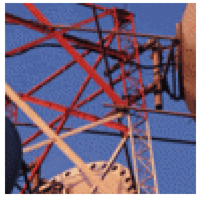
In summary, it assigns these responsibilities and establishes the policy that, “It is the policy of the United States to enhance the security and resilience of the Nation’s **critical infrastructure** and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”

https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

16 Critical Infrastructure Sectors

Chemical

Commercial Facilities


Communication

Critical Manufacturing

Dams

Defense Industrial Base

Emergency Services

Energy

Financial Services

Food and Agriculture

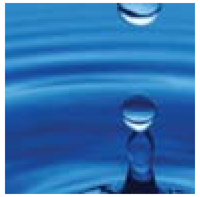
Government Facilities

Healthcare and Public Health

Information Technology

Nuclear Reactors, Materials and Waste

Transportation


Water and Wastewater

https://www.dhs.gov/critical-infrastructure-sectors

What is NIST?

National Institute for Standards and Technology

Founded in 1901, NIST is a non-regulatory federal agency within the **U.S. Department of Commerce**.

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST Cybersecurity Mission:
To implement practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities.

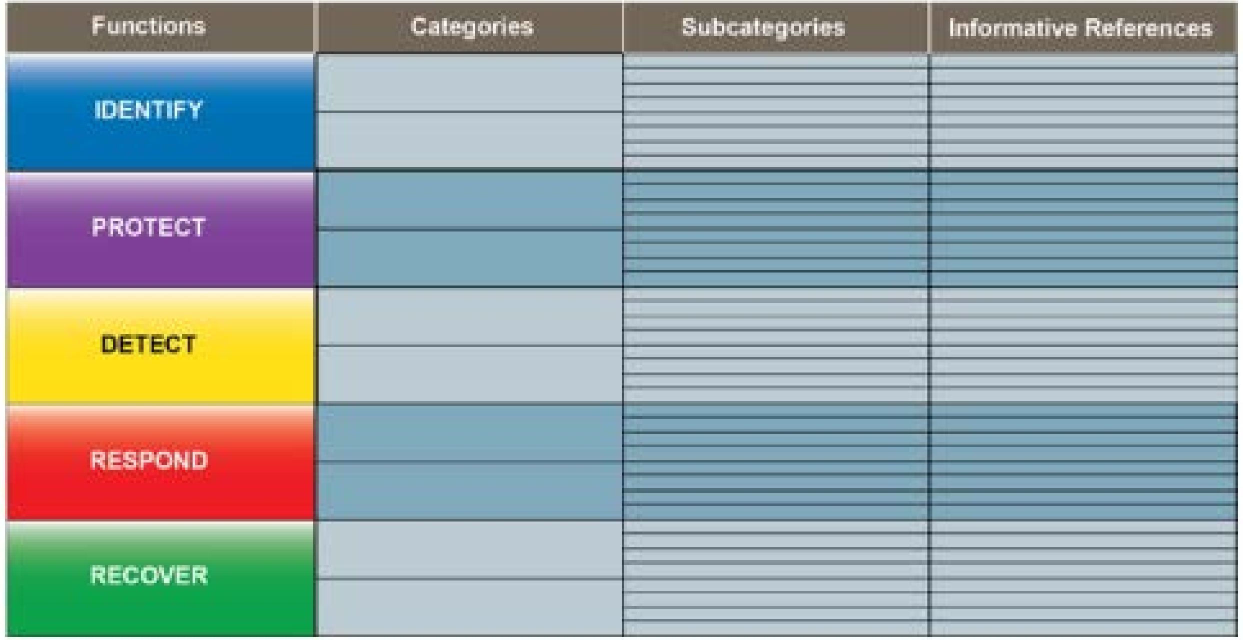
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

https://www.nist.gov/

What is the NIST Framework?

ISA New Orleans Section

- **NIST Framework**
  - Enables organizations to apply the principles and best practices of ***risk management*** to improving the security and resilience of critical infrastructure.
  - Provides ***organization, structure and consistency*** to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today.
  - Consists of three parts
    - Framework Core
    - Framework Implementation Tiers
    - Framework Profile



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Figure 1: Framework Core Structure

https://www.nist.gov/cyberframework

Framework

- Framework Core
- Framework Implementation Tiers
- Framework Profile

Identify

Understanding to manage cybersecurity risk to systems, assets, data, and capabilities

Protect

Safeguards to ensure delivery of critical infrastructure services

Detect

Identify the occurrence of a cybersecurity event

Respond

Action regarding a detected cybersecurity event

Recover

- Maintain plans for resilience
- Restore any capabilities or services

Framework

Framework Core

Framework Implementation Tiers

Framework Profile

Functions	Categories	Subcategories	Informative Reference
IDENTIFY **ID**			
PROTECT **PR**			
DETECT **DE**			
RESPOND **RS**			
RECOVER **RC**			

Framework

IDENTIFY

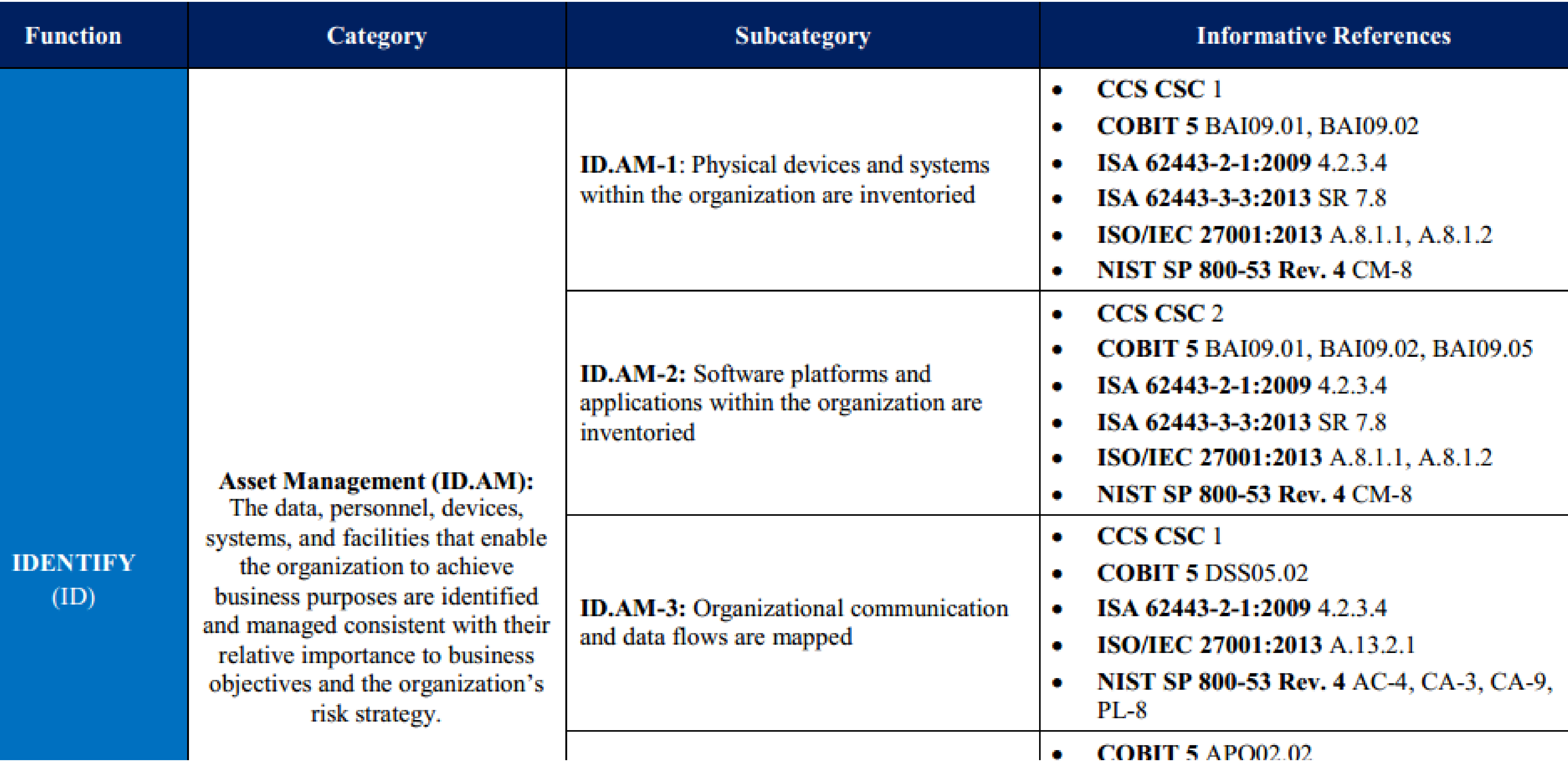
PROTECT

DETECT

RESPOND

RECOVER

Function	Category Identifier	Category
IDENTIFY (ID)	ID.AM	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS 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
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS 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 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
			• **COBIT 5** APO02.02

Framework

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Function	Category Identifier	Category
PROTECT (PR)	PR.AC	Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection Processes and Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology

Framework

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

Function	Category Identifier	Category
DETECT (DE)	DE.AE	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes

Framework

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

Function	Category Identifier	Category
RESPOND (RS)	RS.RP	Response Planning
	RS.CO	Communications
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements

Framework

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Function	Category Identifier	Category
RECOVER (RC)	RC.RP	Recovery Planning
	RC.IM	Improvements
	RC.CO	Communications

Framework

Framework Core

Framework Implementation Tiers

Framework Profile

Cybersecurity Risks

Manage Risks

Partial

Risk Informed

Repeatable

Adaptive

Consideration

- Risk management practices, threat environment, legal & regulatory req., objectives & constraints

	Risk Management Process	Integrated Risk Management Program	External Participation
Tier 1 **Partial**	• Not formalized • Reactive	• Limited awareness • Irregular risk management • Private information	No external collaboration
Tier 2 **Risk Informed**	• Approved practices • Not widely use as policy	• More awareness • Risk-informed, processes & procedures • Adequate resources • Internal sharing	Not formalized to interact & share information
Tier 3 **Repeatable**	• Approved as Policy • Update regularly	• Organization approach • Risk-informed, processes & procedures defined & implemented as intended, and reviewed • Knowledge & skills	• Collaborate • Receive information
Tier 4 **Adaptive**	Continuous improvement	• Risk-informed, processes & procedures for potential events • Continuous awareness • Actively	Actively shares information

Framework

Framework Core

Framework Implementation Tiers

Framework Profile

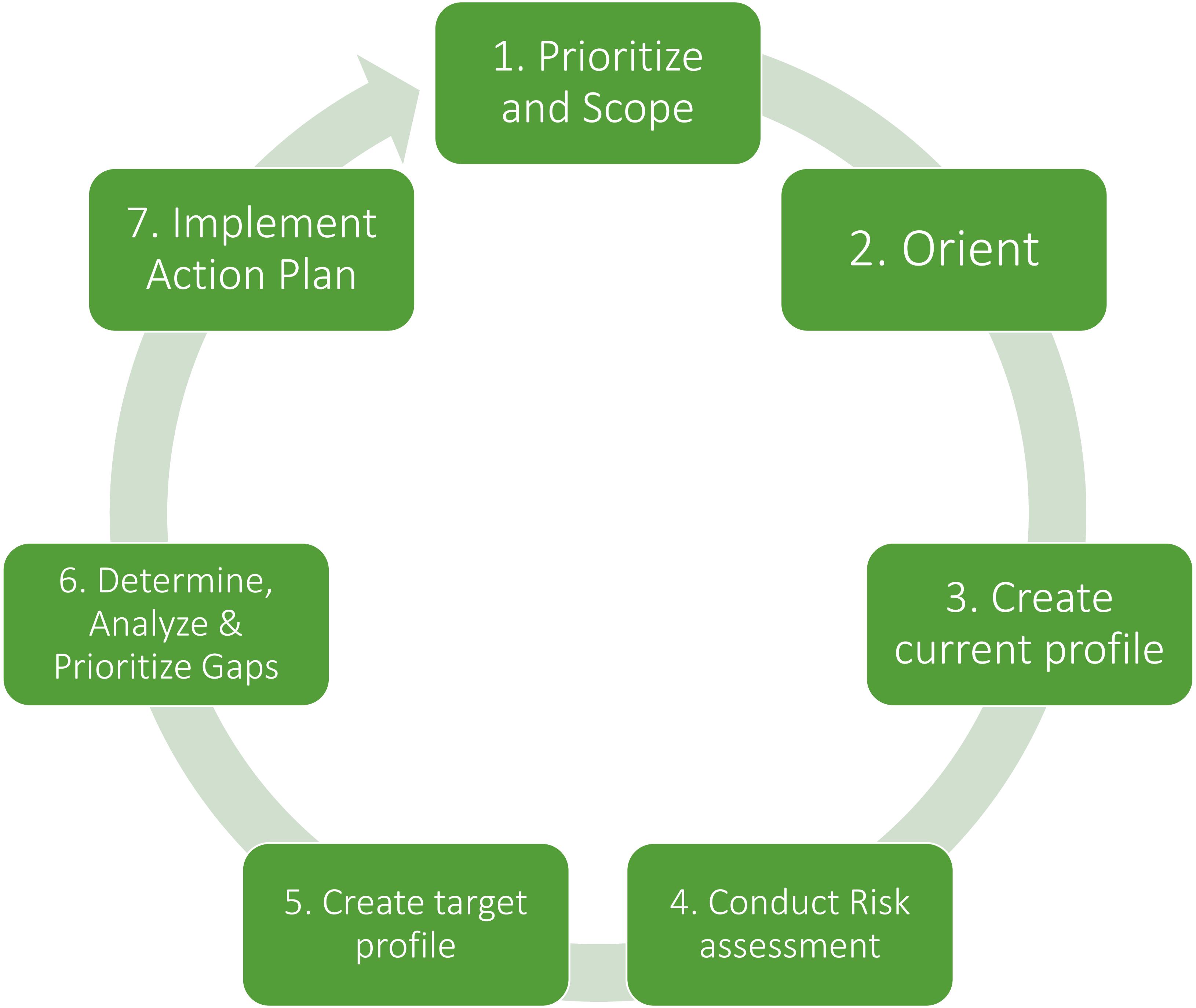
Alignment of Framework Core and business requirements, risk tolerance & resources

Establish roadmap to reduce risk aligned with organizational and sector goals

Describe current and desired state of specific events

Action plan to address gaps

Create or improve a program


1. Prioritize and Scope

2. Orient

3. Create current profile

4. Conduct Risk assessment

5. Create target profile

6. Determine, Analyze & Prioritize Gaps

7. Implement Action Plan

Our Guest Speakers

Gaby Koren
Vice President, Americas

Indegy

Matthew Petrauskas
Regional Account Director

Indegy

ISA™ New Orleans
Section