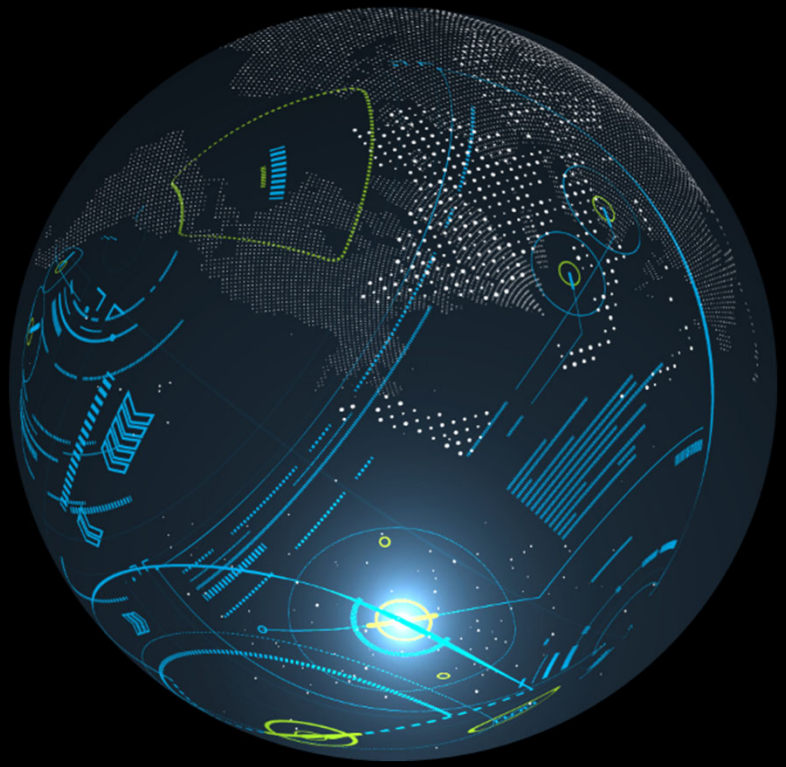
Deloitte.



Managing Risk in the Electric Power Sector

April 2019

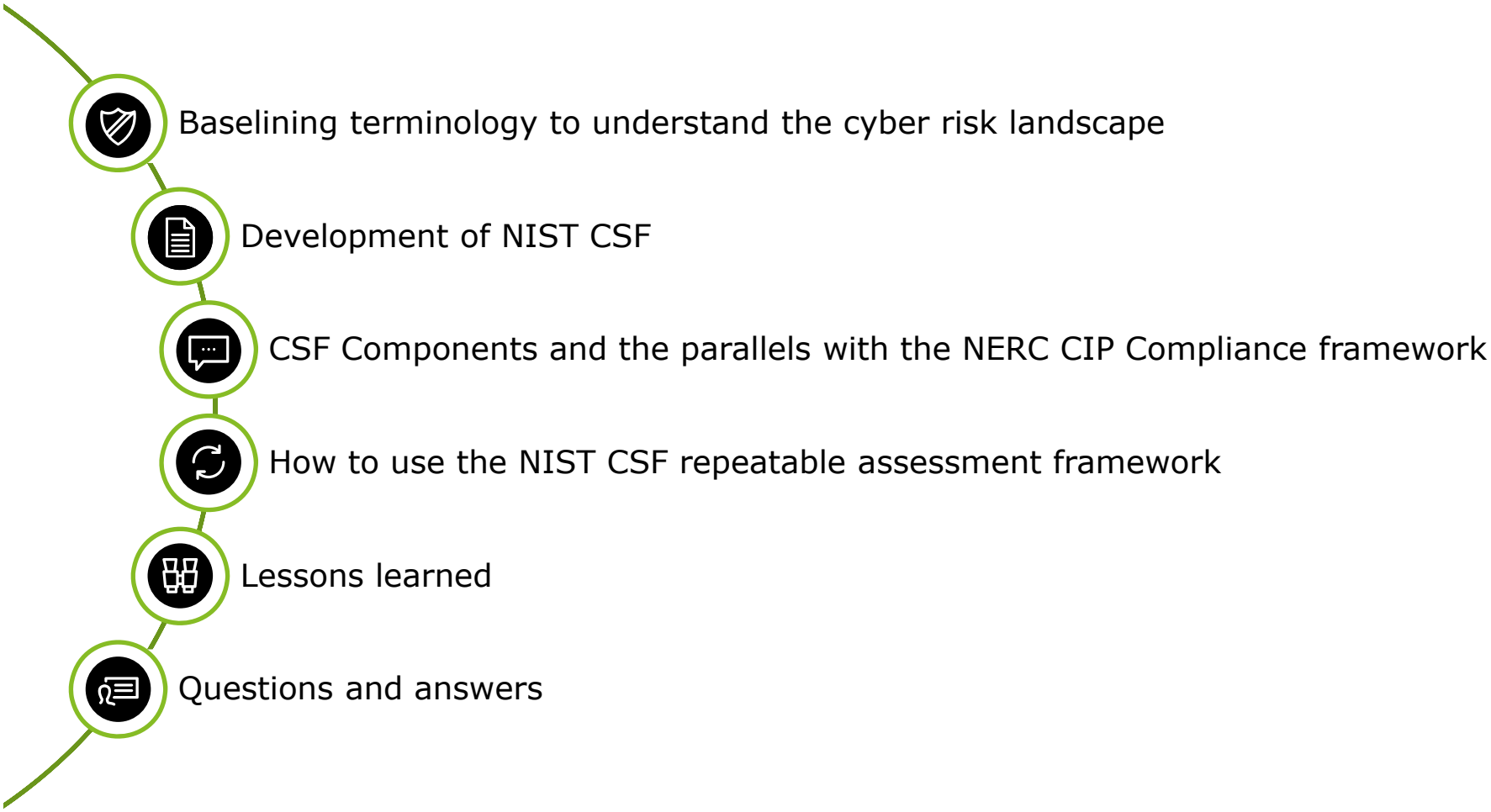
Introduction and objectives

Andrea LeStarge
Senior Manager
Risk & Financial Advisory
Deloitte
414.530.1834
alestarge@deloitte.com

Objectives

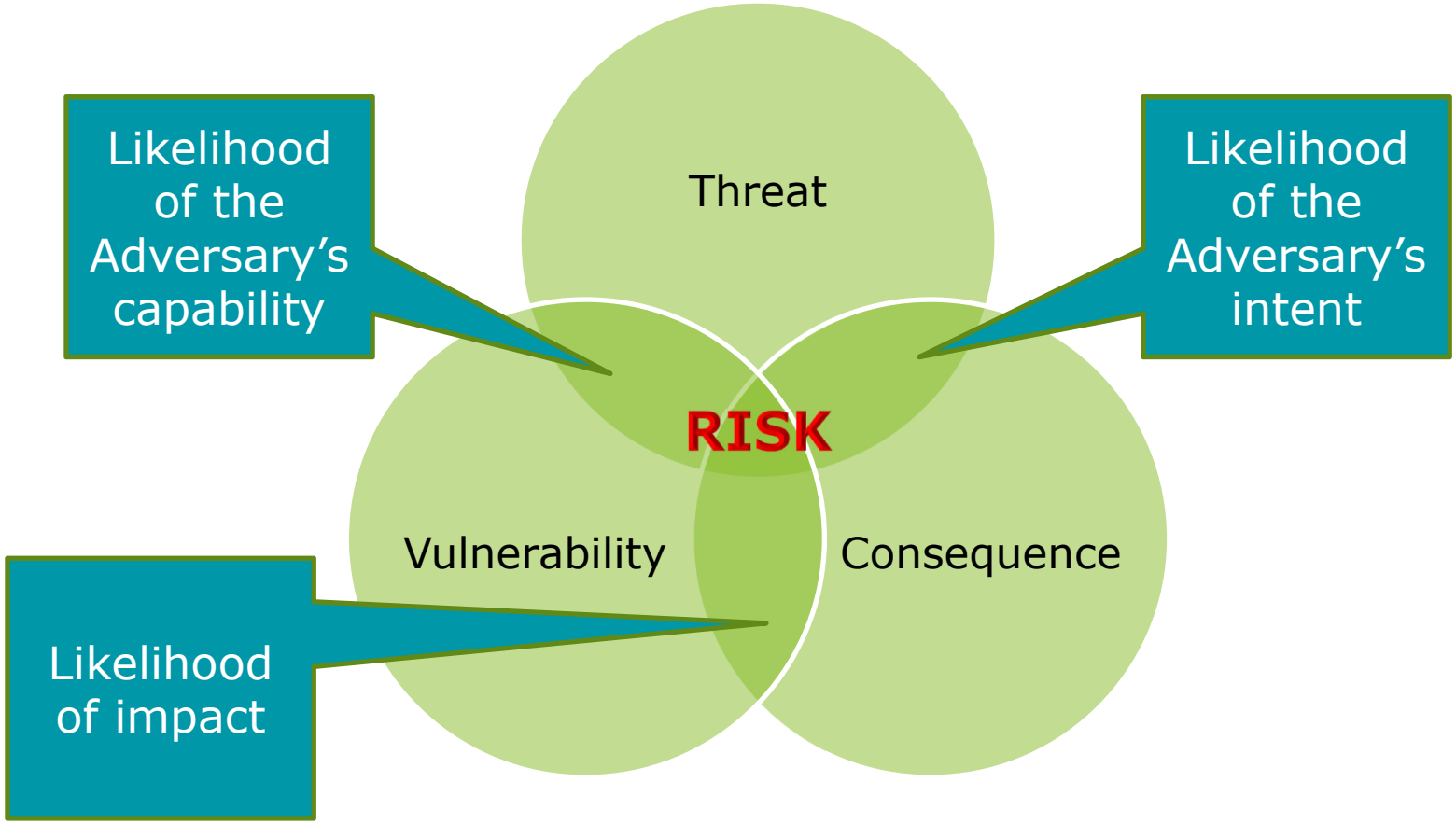
- Baseline on the definition of "risk"
- Introduce methodologies that can help personnel manage cyber risk within the electric power sector
- Engage in a moderated discussion pertaining to the five core functions of the Cybersecurity Framework (CSF) from the National Institute of Standards and Technology (NIST) to share risk-managing activities in the power and utility field

Agenda



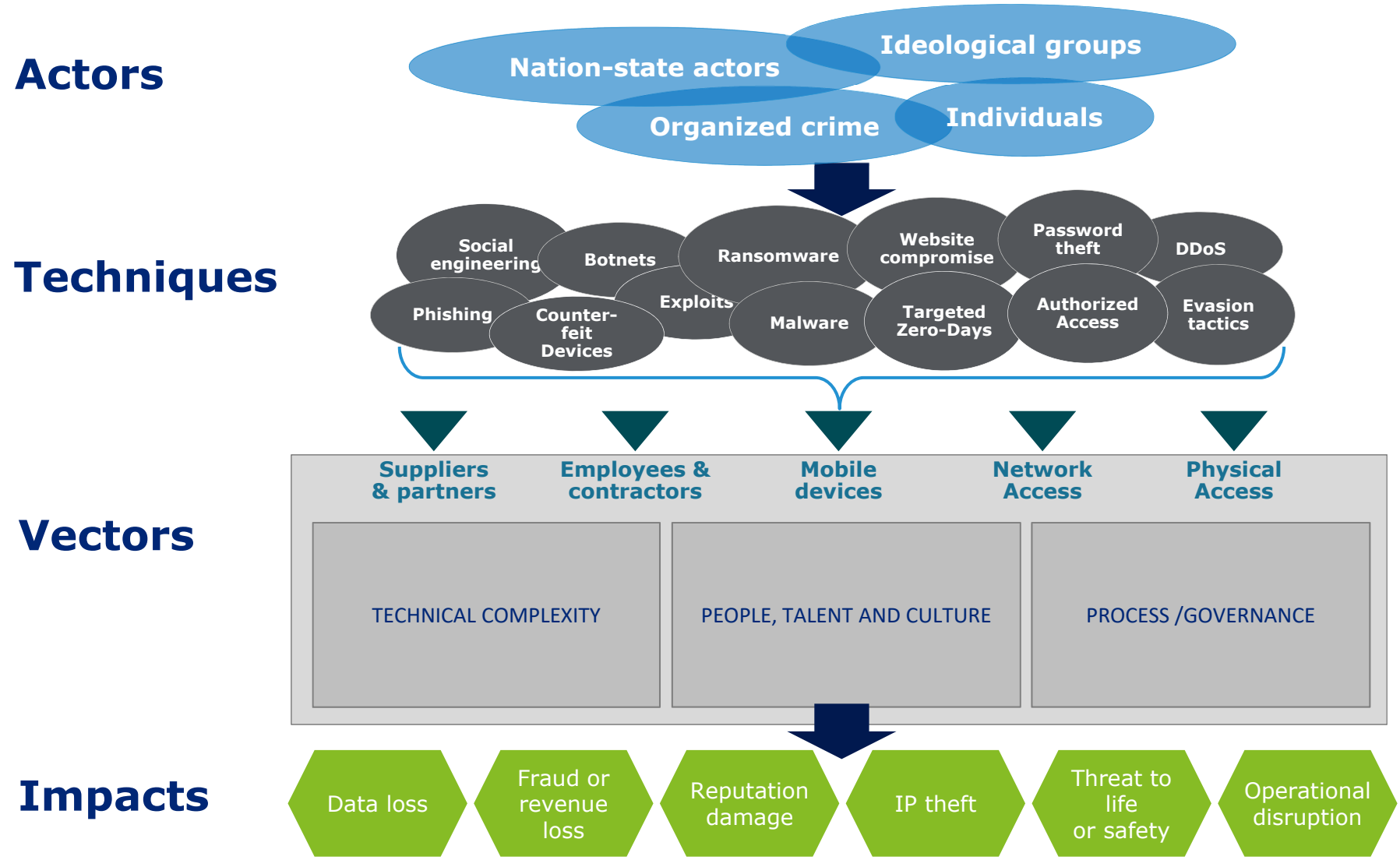
Baselining terminology

For today's discussion, we will refer to the below diagram that visualizes risk as a function of threat, vulnerability and consequence.



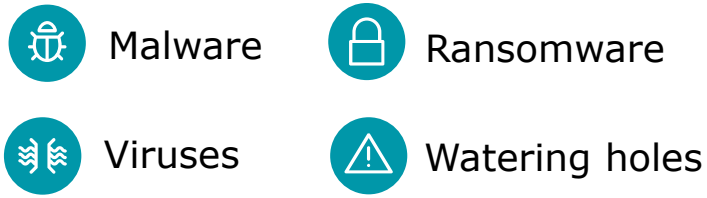
Cyber risk landscape

Looking through the lens of "risk as a function of threat, vulnerability and consequence," we can better understand the cyber risk landscape.



The landscape: Attacks since 2009

Common attack entry points from the supply chain include:



However, threat actors can introduce compromised components into a system, unintentionally or by design, at any point of a system's life cycle.

- 2009 | **Shodan**
  Search engine to find Internet-connected devices (including control system devices)
- July 2010 | **Stuxnet**
  Attack on SCADA control systems irreparably damaged centrifuge equipment at Iranian nuclear facilities
- October 2010 | **Metasploit**
  The security tools was developed to explore system vulnerabilities; hackers began using it to target ICS devices
- August 2012 | **Shamoon**
  Virus destroys data as means to disrupt operations. Hit 15 state and private entities in Saudi Arabia
- December 2015 | **Ukraine Power Grid 1 (BlackEnergy)**
  Attackers deployed SCADA-related plugins to control ICS and turn off power to 230,000 residents of western Ukraine
- 2016 | **Ukraine Power Grid 2 (CrashOverride)**
  Designed to attack electric grids, it took down a Ukrainian transmission-level substation and caused an outage by leveraging legitimate grid operations against the grid itself
- January 2017 | **Shamoon 2**
  This second round of the virus hit a number of state agencies and private sector companies in Saudi Arabia
- August 2017 | **Trisis/Triton**
  Penetrated the safety systems of a petrochemical plant in Saudi Arabia. Designed not just to destroy data or shut down the plant but to sabotage operations and trigger an explosion[1]
- Winter 2018 | **Critical Infrastructure Vendors**
  US-CERT alerts state-sponsored attacks on critical infrastructure vendors [2]

Sources:

[1] Managing cyber risk in the electric power sector, Deloitte Insights, Jan 2019.

[2] US-CERT Alert (TA18-074A), National Cybersecurity and Communications Integration Center, Mar 16, 2018.

Cybersecurity Framework Development

The Framework development process initiated with Executive Order 13636, which was released on February 12, 2013. The Executive Order introduced efforts on the sharing of cybersecurity threat information, and on building a set of current and successful approaches, a framework, for reducing risks to critical infrastructure.

Through this Executive Order, NIST was tasked with the development of a "Cybersecurity Framework"

National Institute of Standards & Technology (NIST) was selected for the task of developing the Framework because they are a non-regulatory Federal agency that acts as an unbiased source of scientific data and practices, including cybersecurity practices.

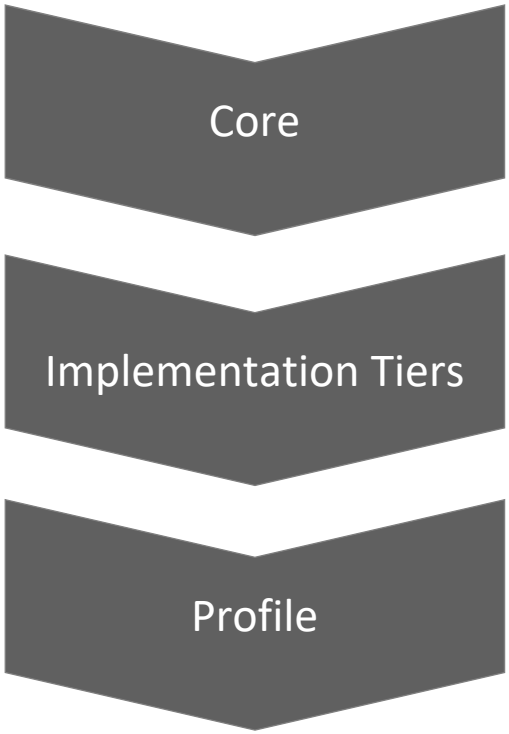
NIST published the Cybersecurity Framework (CSF) version 1.0 on February 12, 2014 after a year-long collaborative effort with stakeholders in the critical infrastructure[1] sector. The latest version (version 1.1) was released on April 16, 2018.

CSF leverages elements of existing well-known risk management frameworks, processes, and guidelines (i.e., COBIT, ISA, ISO 27001 and NIST SP800/53).

[1] Critical infrastructure is defined in the U.S. Patriot Act of 2001 as, "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Cybersecurity Framework Components

The framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts as shown below. The components reinforce the connection between business/mission drivers and cybersecurity activities.



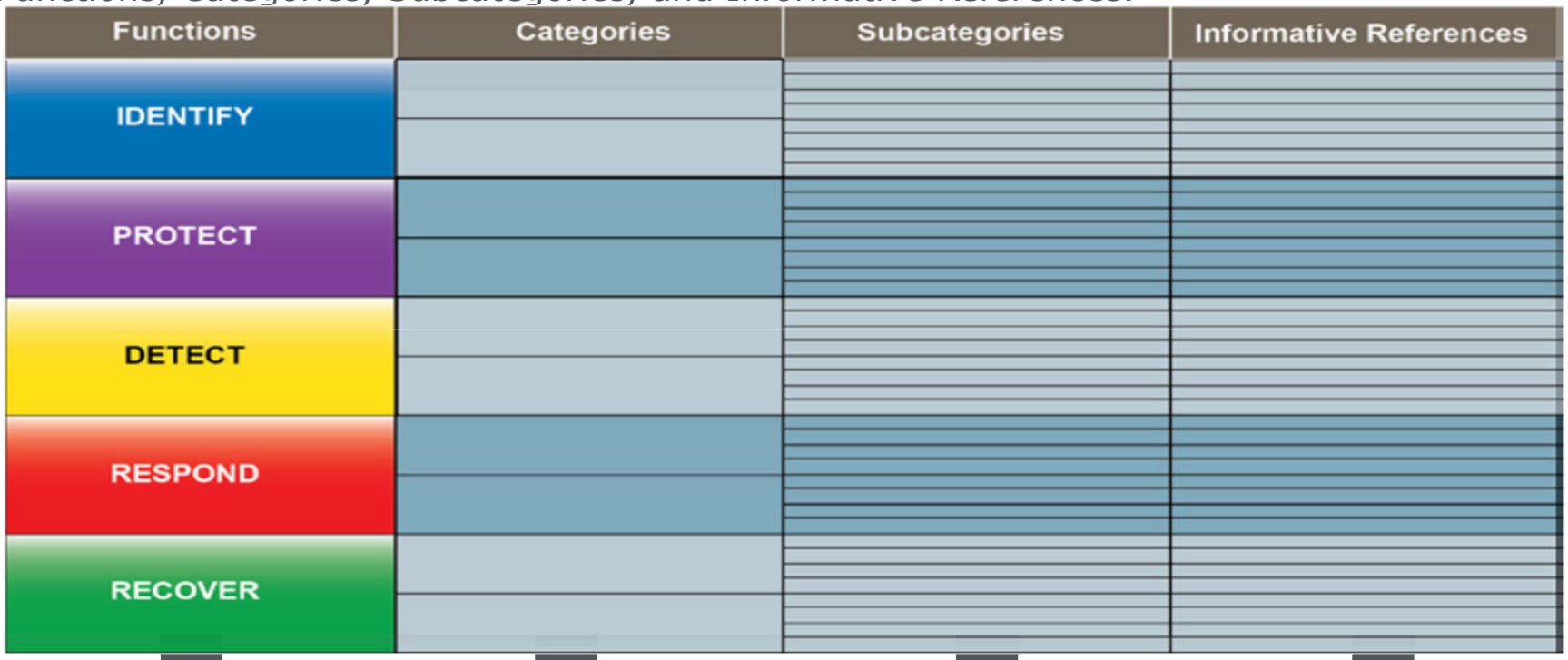
- Cybersecurity activities and informative references, organized around particular outcomes
- Enables communication of cybersecurity risks across an organization

- Describes the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive)

- 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

The core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. It comprises four elements: Functions, Categories, Subcategories, and Informative References.



Aids an organization in expressing its management of cybersecurity risk by organizing information

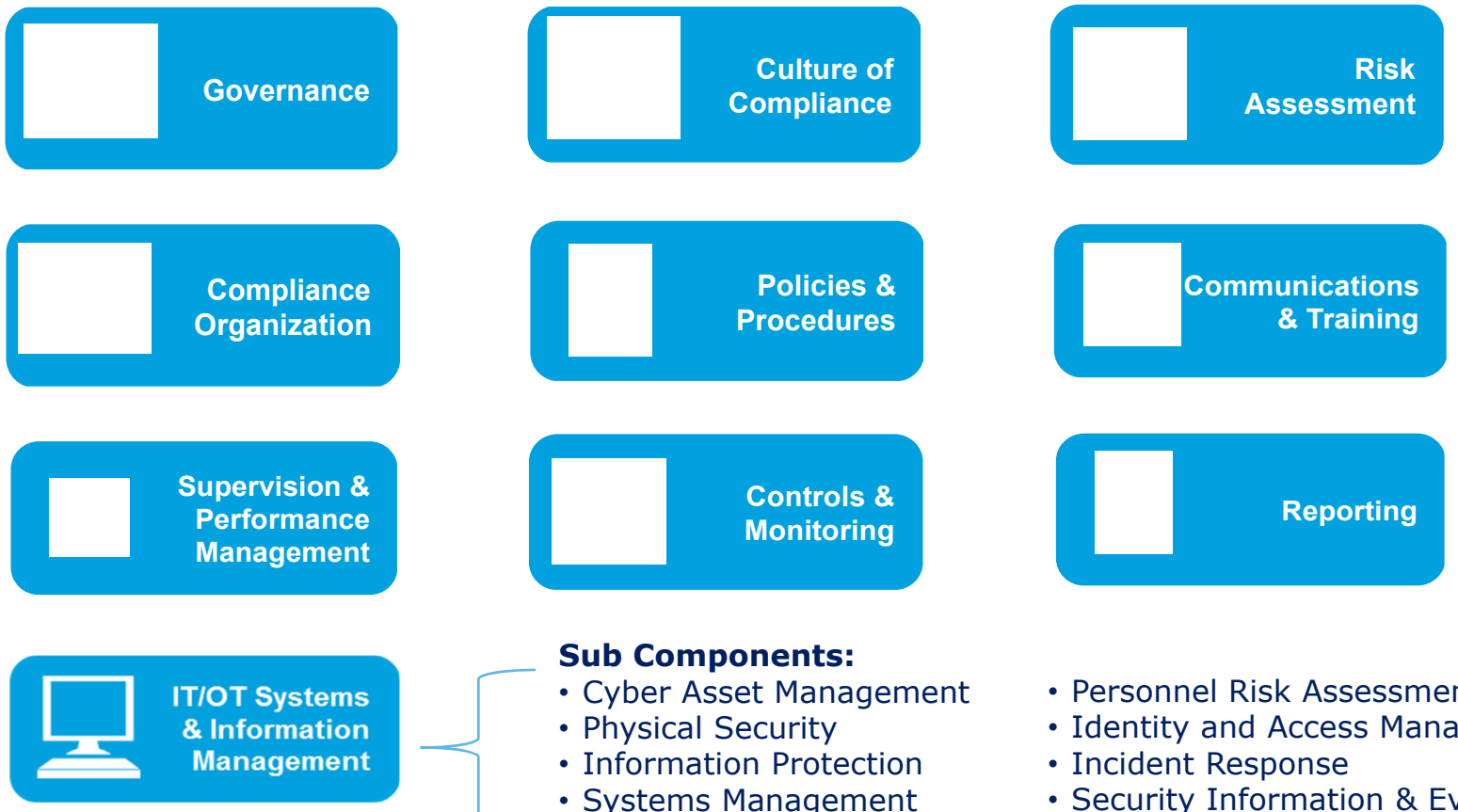
Subdivisions of a function into groups of cybersecurity outcomes closely tied to programs and particular activities

Divides a category into specific outcomes of technical and/or management activities

Specific sections of standards, guidelines, and practices common among critical infrastructure sectors

Parallels with the NERC CIP Compliance framework

The following NERC CIP Compliance framework defines the program elements necessary to implement and maintain an effective program:



Sub Components:

- Cyber Asset Management
- Physical Security
- Information Protection
- Systems Management
- Production Change Management
- Personnel Risk Assessment
- Identity and Access Management
- Incident Response
- Security Information & Event Management
- Vulnerability Management

Moderated discussion

How would you answer each of the five questions below?

1. **What processes and assets need protection?**
2. **What safeguards or countermeasures are available?**
3. **What techniques can identify security incidents?**
4. **What activities can help contain the impacts of incidents?**
5. **What activities are required to restore capabilities?**

Framework Core (cont'd)

Functions are to be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

Function	Category	The Challenge	Physical Controls	Cyber Controls
Identify	Asset Management	**What processes and assets need protection?**		
	Business Environment			
	Governance			
	Risk Assessment			
	Risk Management Strategy			
	Supply Chain Management			
Protect	Access Control	**What safeguards or countermeasures are available?**		
	Awareness and Training			
	Data Security			
	Info Protection Process & Procedure			
	Maintenance			
	Protective Technology			
Detect	Anomalies and Events	**What techniques can identify cybersecurity incidents?**		
	Security Continuous Monitoring			
	Detection Processes			
Respond	Response Planning	**What activities can help contain the impacts of incidents?**		
	Communications			
	Analysis			
	Mitigation			
	Improvements			
Recover	Recovery Planning	**What activities are required to restore capabilities?**		
	Improvements			
	Communications			

Framework Core (cont'd)

Functions are to be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

Function	Category	The Challenge	Physical Controls	Cyber Controls
Identify	Asset Management	What processes and assets need protection?		
	Business Environment			
	Governance			
	Risk Assessment			
	Risk Management Strategy			
	Supply Chain Management			

Framework Core (cont'd)

Functions are to be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

Function	Category	The Challenge	Physical Controls	Cyber Controls
Protect	Access Control	What safeguards or countermeasures are available?		
	Awareness and Training			
	Data Security			
	Info Protection Process & Procedure			
	Maintenance			
	Protective Technology			

Framework Core (cont'd)

Functions are to be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

Function	Category	The Challenge	Physical Controls	Cyber Controls
Detect	Anomalies and Events	What techniques can identify cybersecurity incidents?		
	Security Continuous Monitoring			
	Detection Processes			

Framework Core (cont'd)

Functions are to be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

Function	Category	The Challenge	Physical Controls	Cyber Controls
Respond	Response Planning	What activities can help contain the impacts of incidents?		
	Communications			
	Analysis			
	Mitigation			
	Improvements			

Framework Core (cont'd)

Functions are to be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

Function	Category	The Challenge	Physical Controls	Cyber Controls
Recover	Recovery Planning	What activities are required to restore capabilities?		
	Improvements			
	Communications			

Framework Implementation Tiers

Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. An organization's current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, and supply chain cybersecurity requirements are considered while determining the tiers.

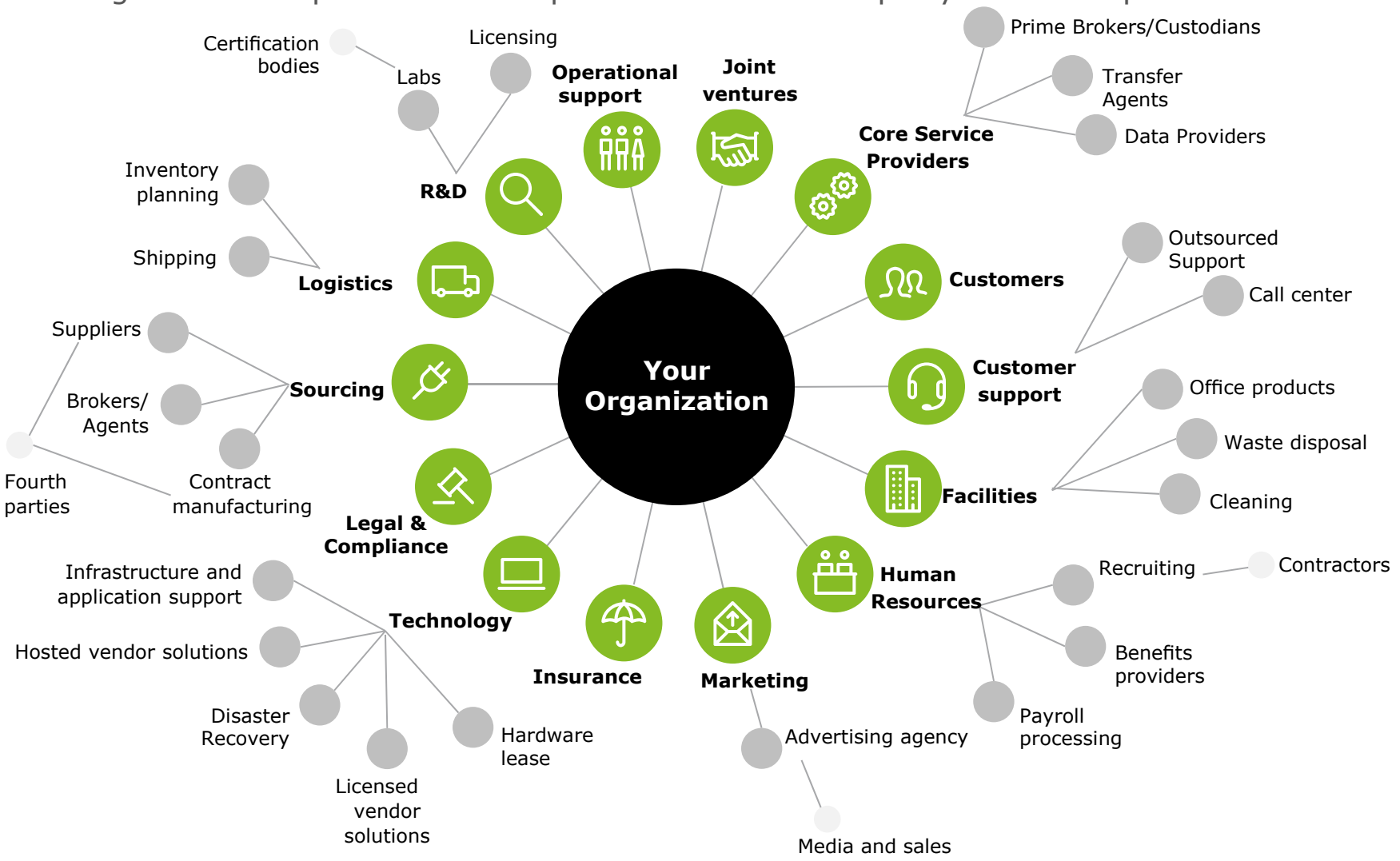
	Tier 1: Partial	**Tier 2: Risk Informed**	**Tier 3: Repeatable**	**Tier 4: Adaptable**
Risk Management Process The degree to which risk management processes are applied in alignment with organizational risk objectives, changes in business/mission requirements and a changing threat and technology landscape.	• Not formalized • Ad hoc • Prioritization is not informed	• Formalized, but no organizational-wide policy • Directly informed	• Formal • Regularly updated	• Incorporates: ○ Predictive indicators ○ Lessons Learned
Integrated Risk Management Program Definition and implementation of risk-informed policies, processes, and procedures to enable personnel to possess the knowledge and skill to perform their appointed cybersecurity roles and responsibilities.	• Irregular, case-by-case basis	• Regular, but no organizational-wide approach	• Consistent, organization-wide approach	• Cybersecurity risk management is part of the organization's culture
External Participation Understanding of an organization's role, dependencies, and dependents in the larger ecosystem by collaborating with and receiving information from other entities regularly that complements internally generated information, and sharing information with other entities	• Lack of: ○ Ecosystem understanding ○ Collaboration	• Dependencies or dependents known, but not both • Internal informal sharing	• Both dependencies and dependents are known • Internal and external information sharing	• Generates prioritized information • Communicates proactively

Framework Profile

The Framework Profile is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. They can be used to describe the current state or the desired target state of specific cybersecurity activities.

Lessons learned: The extended enterprise does not operate in isolation

Your organization depends on a complex network of third-party relationships.



Lessons learned: Known cyber events in utilities and other critical infrastructure

Key themes from all cyber attacks arise, but range from cyber program management and governance to technical architecture considerations. Below are 10 of the most common lessons.

1

- No organization or industry is immune to the threat of a cyber attack

2

- Minimize potential disruptions in advance of the next cyber attack, companies should review their cyber risk management strategies periodically

3

- Even relatively unsophisticated attacks can cause significant damage or operational disruption under the right conditions

4

- Educate employees and contractors on a regular basis to be always vigilant and increase awareness on potential cyber threats

5

- Conduct periodic audit on critical infrastructure and always be on the lookout for opportunities to improve security

6

- Apply network segmentation and multi-factor authentication on all systems containing sensitive data

7

- Implement continuous monitoring on critical devices (e.g. ICS/SCADA) to detect anomalous activities

8

- Control applications to reduce the risk of malware-based attacks

9

- Conduct frequent simulated cyber attacks (e.g. phishing awareness exercise, tabletop exercises) at every level of the organization

10

- Back up data vigilantly to minimize work disruption

Source:#WannaCry: Lessons Learned and Implications, 2017, Mash; Lessons Learned from a Ransomware Attack, 2016, Interset; Lessons from Frontlines of Power Utility Attacks, 2016, Tripwire; 5 Key lessons Learned from Critical Infrastructure Cyber Attacks, RedTeam Security Consulting

Questions & Answers

Deloitte.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.