# NIST CYBERSECURITY FRAMEWORK

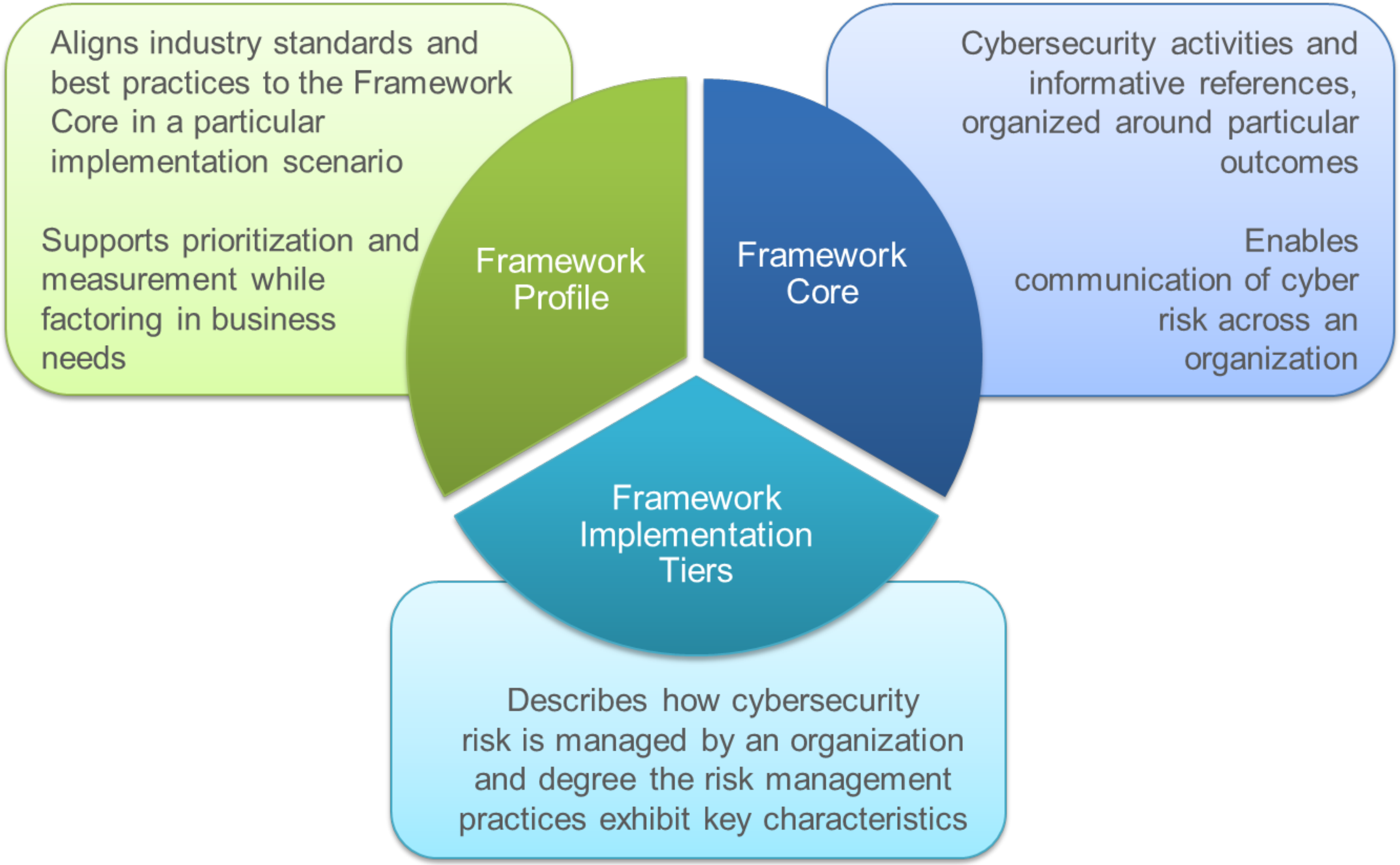
# KEY CYBER SECURITY FRAMEWORK ATTRIBUTES

## PRINCIPLES OF THE CURRENT AND FUTURE VERSIONS OF FRAMEWORK

- **Common and accessible language**
  - Understandable by many professionals
- **It’s adaptable to many technologies$^{1.1}$, lifecycle phases$^{1.1}$, sectors and uses**
  - Meant to be customized
- **It’s risk-based**
  - A Catalog of cybersecurity outcomes
  - Does not provide how or how much cybersecurity is appropriate
- **It’s meant to be paired**
  - Take advantage of great pre-existing things
- **It’s a living document**
  - Enable best practices to become standard practices for everyone
  - Can be updated as technology and threats change
  - Evolves faster than regulation and legislation
  - Can be updated as stakeholders learn from implementation

**Source:** *The Framework for Improving Critical Infrastructure Cybersecurity, April 2018,* *https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview*

# CYBERSECURITY FRAMEWORK OVERVIEW



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

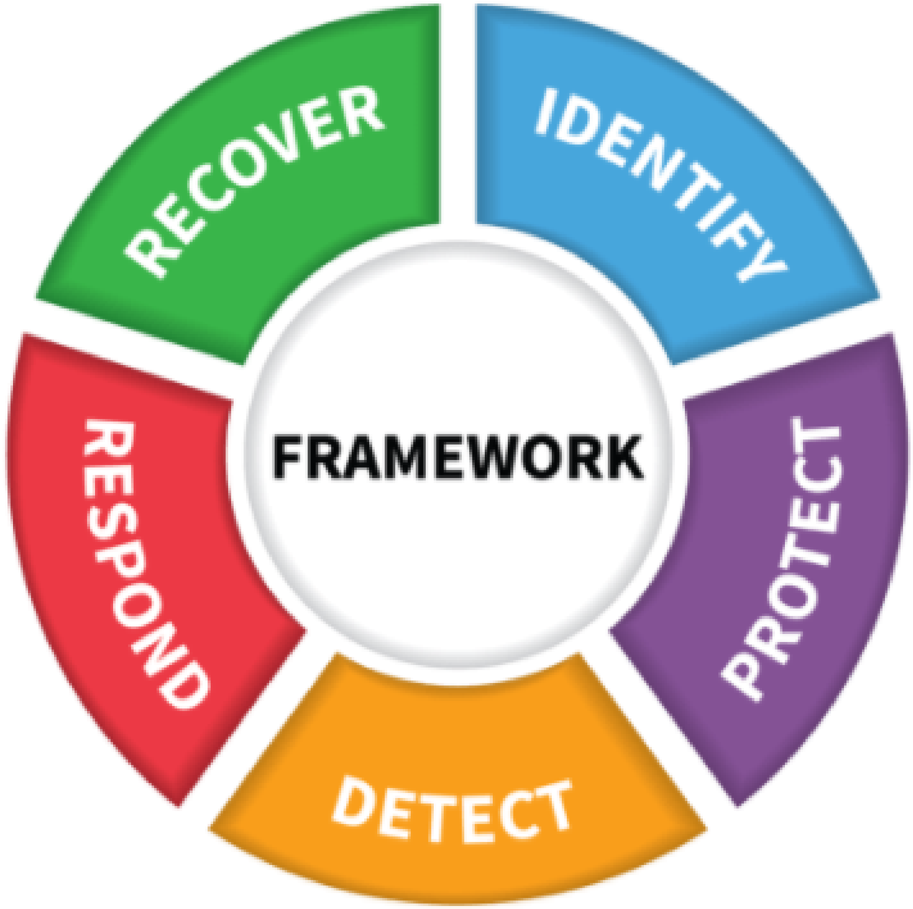
Enables communication of cyber risk across an organization

Framework Implementation Tiers

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

**Source:** *The Framework for Improving Critical Infrastructure Cybersecurity, April 2018, https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview*

# THE FIVE FUNCTIONS OF THE FRAMEWORK



# CYBERSECURITY FRAMEWORK OVERVIEW
## FRAMEWORK CORE

### *Categories and Subcategories*

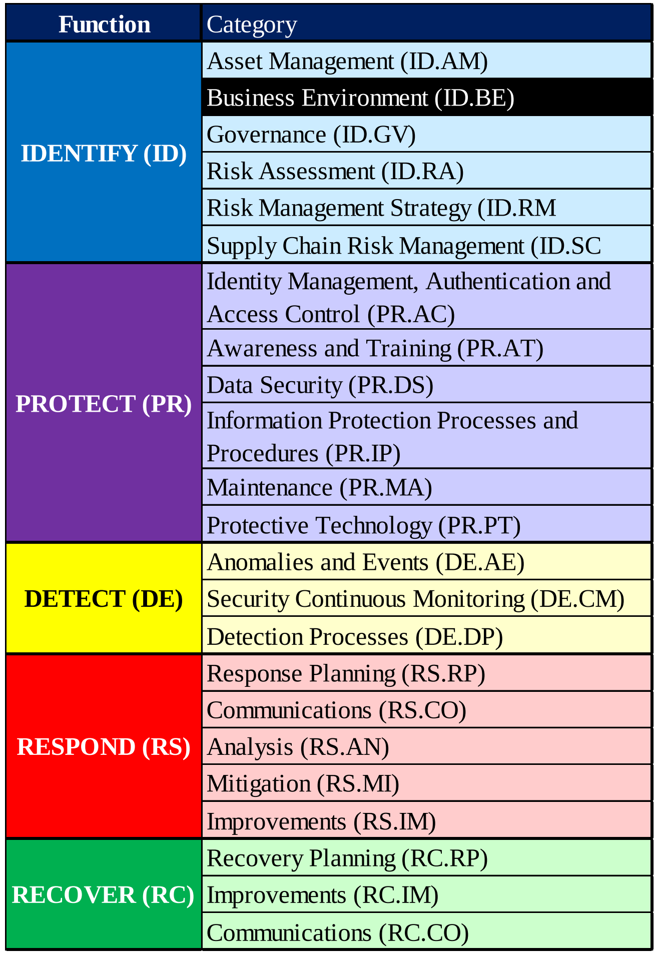
What processes and assets need protection?

What safeguards are available?

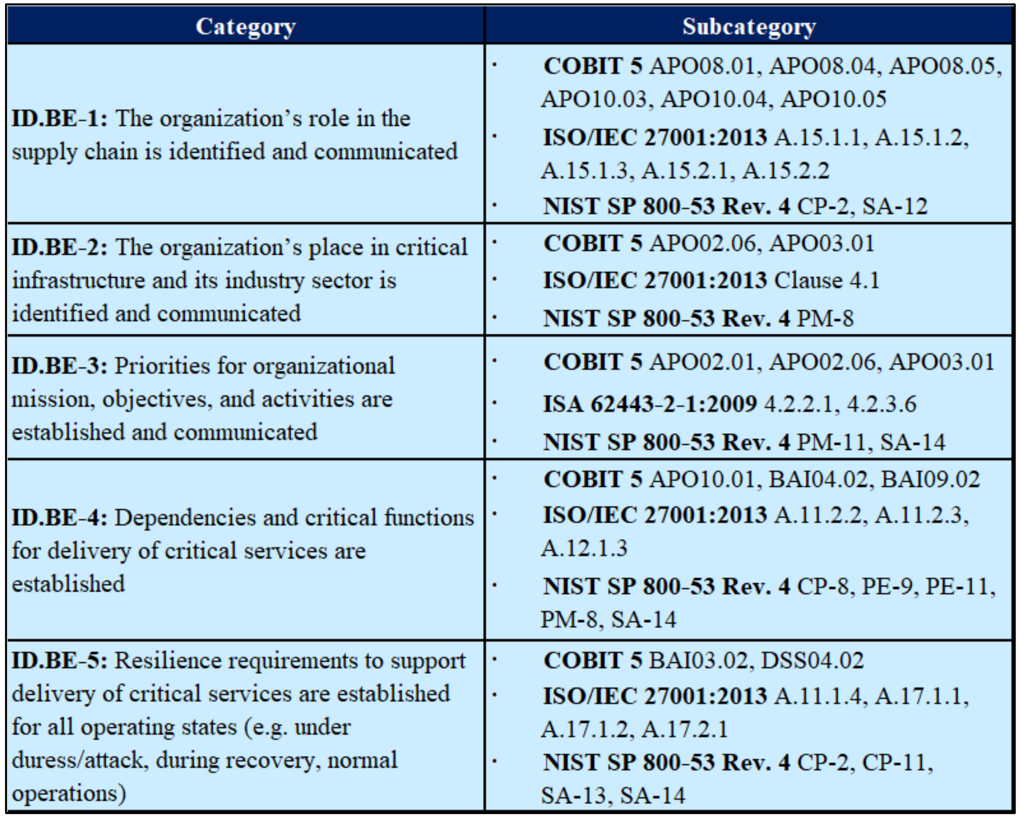
What techniques can identify incidents?

What techniques can contain impacts of incidents?

What techniques can restore capabilities?



| Function | Category |
|---|---|
| IDENTIFY (ID) | Asset Management (ID.AM) |
| | Business Environment (ID.BE) |
| | Governance (ID.GV) |
| | Risk Assessment (ID.RA) |
| | Risk Management Strategy (ID.RM |
| | Supply Chain Risk Management (ID.SC |
| PROTECT (PR) | Identity Management, Authentication and Access Control (PR.AC) |
| | Awareness and Training (PR.AT) |
| | Data Security (PR.DS) |
| | Information Protection Processes and Procedures (PR.IP) |
| | Maintenance (PR.MA) |
| | Protective Technology (PR.PT) |
| DETECT (DE) | Anomalies and Events (DE.AE) |
| | Security Continuous Monitoring (DE.CM) |
| | Detection Processes (DE.DP) |
| RESPOND (RS) | Response Planning (RS.RP) |
| | Communications (RS.CO) |
| | Analysis (RS.AN) |
| | Mitigation (RS.MI) |
| | Improvements (RS.IM) |
| RECOVER (RC) | Recovery Planning (RC.RP) |
| | Improvements (RC.IM) |
| | Communications (RC.CO) |

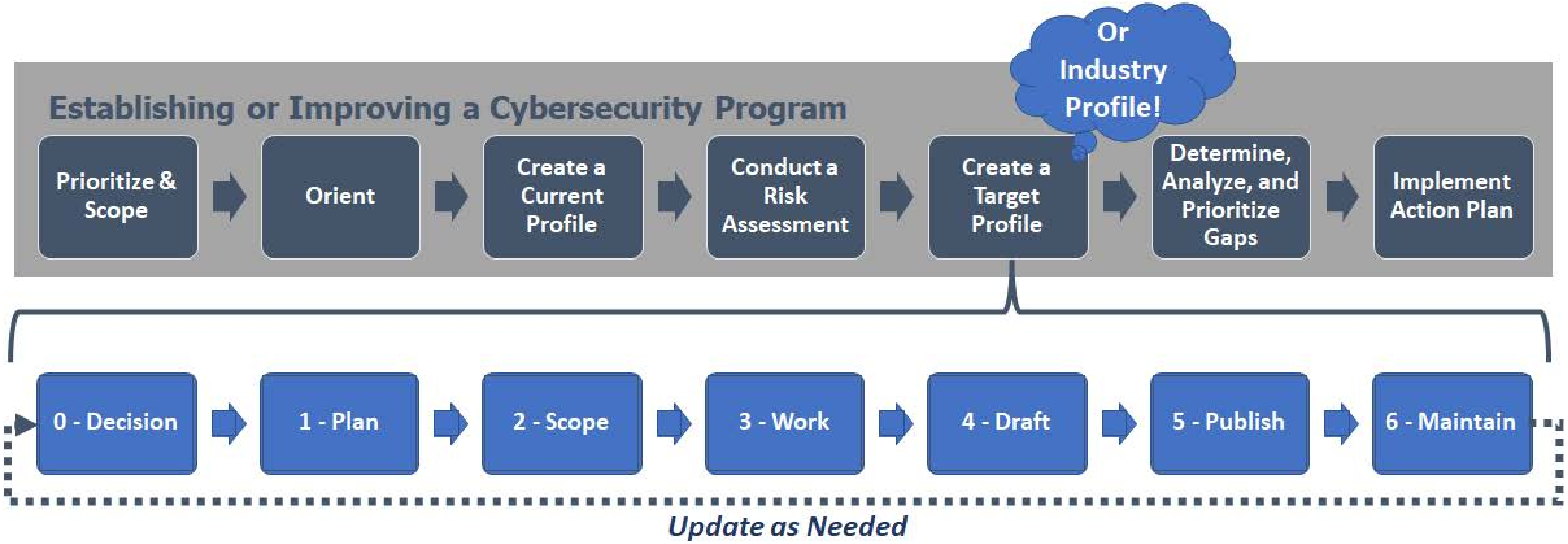


| Category | Subcategory |
|---|---|
| **ID.BE-1:** The organization's role in the supply chain is identified and communicated | · **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05<br>· **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2<br>· **NIST SP 800-53 Rev. 4** CP-2, SA-12 |
| **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | · **COBIT 5** APO02.06, APO03.01<br>· **ISO/IEC 27001:2013** Clause 4.1<br>· **NIST SP 800-53 Rev. 4** PM-8 |
| **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | · **COBIT 5** APO02.01, APO02.06, APO03.01<br>· **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6<br>· **NIST SP 800-53 Rev. 4** PM-11, SA-14 |
| **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established | · **COBIT 5** APO10.01, BAI04.02, BAI09.02<br>· **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3<br>· **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14 |
| **ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) | · **COBIT 5** BAI03.02, DSS04.02<br>· **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1<br>· **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14 |

**Source:** *The Framework for Improving Critical Infrastructure Cybersecurity, April 2018, https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview*

# FRAMEWORK SEVEN STEP PROCESS

## GAP ANALYSIS USING FRAMEWORK PROFILES



Establishing or Improving a Cybersecurity Program

Prioritize & Scope → Orient → Create a Current Profile → Conduct a Risk Assessment → Create a Target Profile → Determine, Analyze, and Prioritize Gaps → Implement Action Plan

Or Industry Profile!

0 - Decision → 1 - Plan → 2 - Scope → 3 - Work → 4 - Draft → 5 - Publish → 6 - Maintain

*Update as Needed*

**Source:** *NCCoE, How To: Develop a Cybersecurity Framework Profile, NIST Cybersecurity Risk Management Conference 2018*

# CONNECTED VEHICLE PILOT DRAFT PROFILE

# DISCUSSION OF MISSION OBJECTIVES

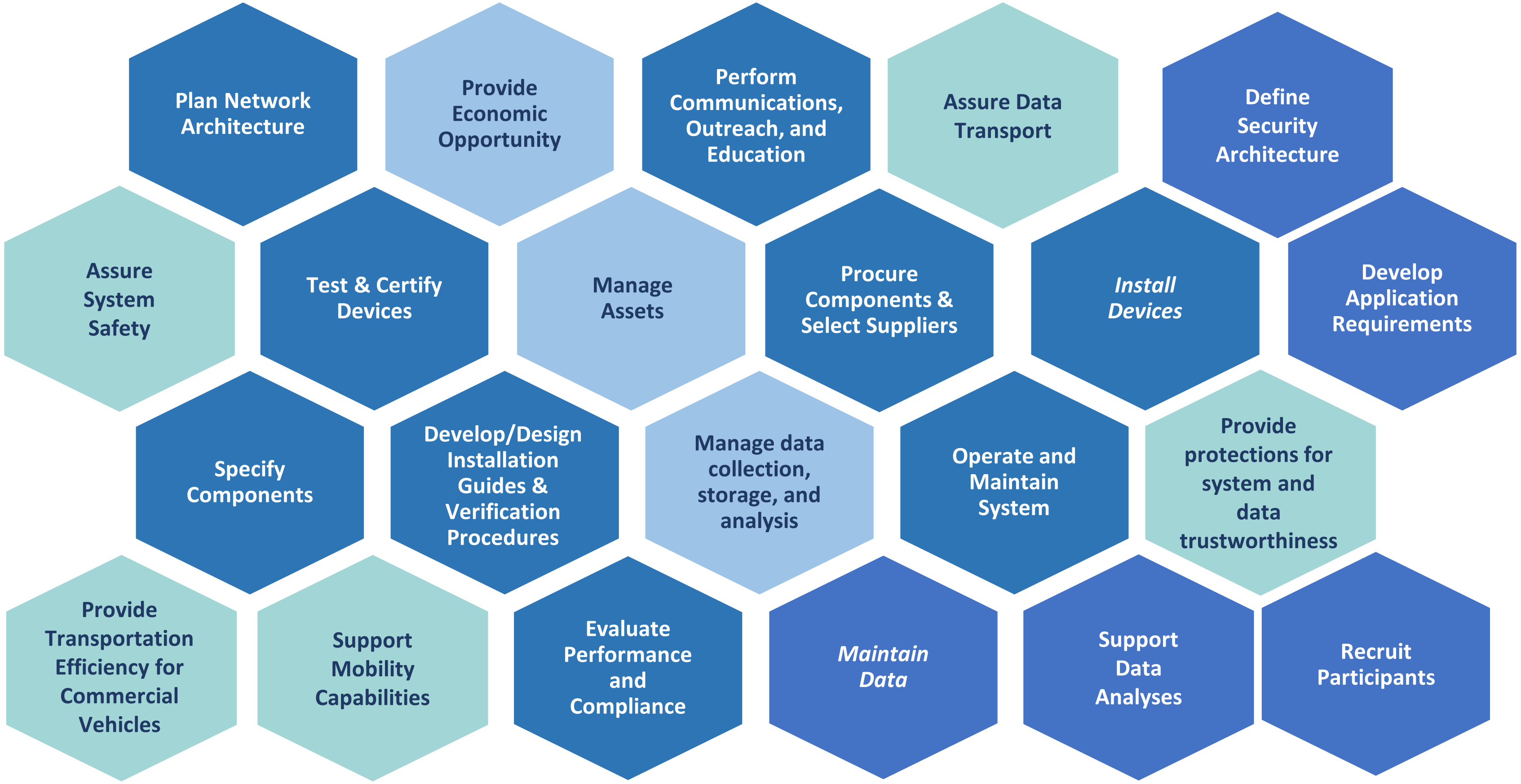
- **Guiding Questions**

- **Transposing Mission to Cyber**
  - What are threats to achievement of those Mission Objectives?
  - What sort of damages does it cause when those Mission Objectives are disrupted?
  - What are your most important assets for a given Mission Objective?
  - Where does physical infrastructure effect cyber infrastructure and vice versa?

- **Which Categories are Most Important?**
  - Pick top three Categories for each Mission Objective
    - *Rank them 1, 2, 3*
  - Pick the highest priority Category for each Function for each Mission Objective (even if your top 3 don't appear in that Function)
    - *Label with an H*

# EXAMPLES OF MISSION OBJECTIVES

## Determine Commonalities Among Business Functions


Plan Network Architecture
Provide Economic Opportunity
Perform Communications, Outreach, and Education
Assure Data Transport
Define Security Architecture
Assure System Safety
Test & Certify Devices
Manage Assets
Procure Components & Select Suppliers
*Install Devices*
Develop Application Requirements
Specify Components
Develop/Design Installation Guides & Verification Procedures
Manage data collection, storage, and analysis
Operate and Maintain System
Provide protections for system and data trustworthiness
Provide Transportation Efficiency for Commercial Vehicles
Support Mobility Capabilities
Evaluate Performance and Compliance
*Maintain Data*
Support Data Analyses
Recruit Participants

**KEY:** All Consensus | AACVTE | Pilots