# CYBERSECURITY FOR STARTUPS AND SMALL BUSINESSES

## OVERVIEW OF CYBERSECURITY FRAMEWORKS

WILLIAM (THE GONZ) FLINN

*M.S. INFORMATION SYSTEMS SECURITY MANAGEMENT; COMPTIA SECURITY+, I-NET+, NETWORK+; CERTIFIED PATCHLINK ENGINEER*

ENTERPRISE INFORMATION SYSTEMS SECURITY MANAGER

HTTPS://WWW.LINKEDIN.COM/IN/WILLIAMFLINN/
WFLINN.ITISSM@GMAIL.COM

# INTRODUCTION

“Cybersecurity is critical to any business enterprise, no matter how small. However, leaders of small and midsize businesses (SMB) often do not know where to begin, given the scope and complexity of the issue in the face of a small staff and limited resources.”

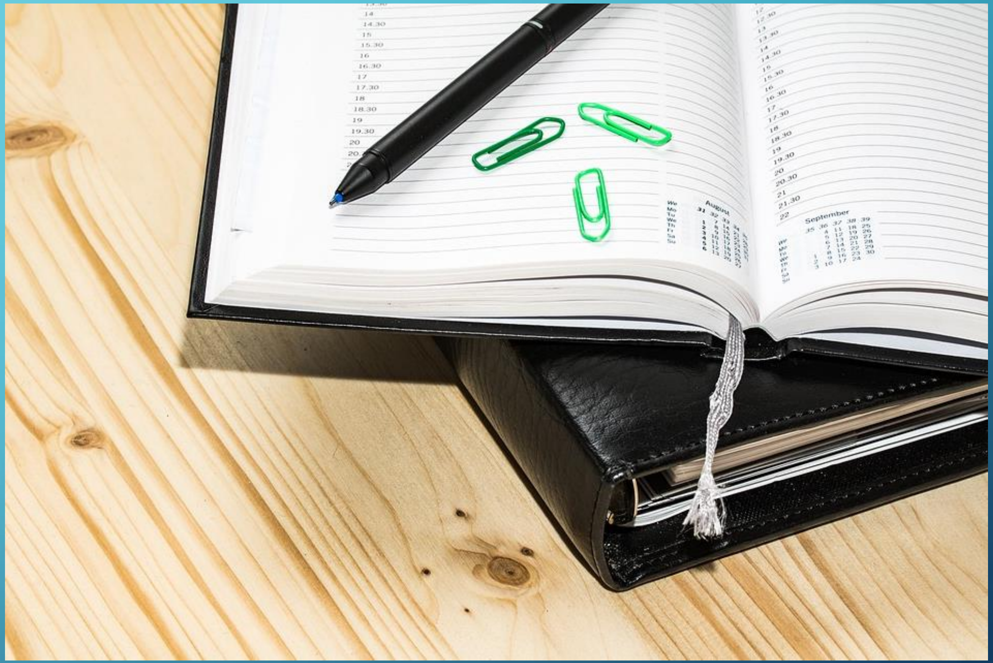
US-CERT

“Every Small Business Should Use the NIST Cybersecurity Framework”

Ola Sage, CEO, e-Managment

# AGENDA

- Cybersecurity and Small Business (The what, why, how)
- Formalized Frameworks and Risk Management
- Cybersecurity Framework
- Cyber Resilience Review (CRR)
- Wrapping It All Up
- What You Can Do
- References and Resources
- Q&A



# CYBERSECURITY AND SMALL BUSINESS

- Balance between securing your assets/information and being able to still do business.
- Analyzing risk and implementing meaningful protections.
  - Don't protect a $10 dollar horse with a $100 dollar fence.
  - This doesn't have to mean performing huge amounts of "mental gymnastics" to get it done.
  - This doesn't have to be complicated or expensive.
- Getting to "Yes" instead of cybersecurity always being "NO!"
- Security should be baked in, not sprinkled on.

# CYBERSECURITY AND STARTUPS

- You have a golden opportunity to bake in security from the very beginning!
- It’s easier to build in security from the start than to try to add in later.

**Cybersecurity for Startups**

# WHY DO WE NEED TO PROTECT SMALL BUSINESS IT ASSETS?

- Practically everything is connected to the Internet.
- Internet of Things (IoT) devices abound.
- Personal data, healthcare data, financial data, manufacturing data, customer account data, credit card data… all need to be protected.
- Foreign entities aren’t just after our military secrets!
  - They want trade secrets, manufacturing secrets, marketing secrets… and not just from the government and large corporations!
- Misuse of company computing assets can compromise security as well as the company’s reputation, and possibly have legal implications.

# SO HOW DO WE PROTECT ALL THIS STUFF?

- Utilize a formalized security framework to measure consistency and effectiveness:
  - Cybersecurity Framework developed by NIST
  - Cyber Resilience Review method developed by DHS
- Perform a risk analysis.
- Have a formalized security plan and policies.
- Implement security “controls” to ensure consistency and best practices.
- Document what you will do to meet each control.
- Do what you say you will do for each control.
- Self-assess each control.
- Have a third party periodically assess your controls.

# WHERE DOES SMALL BUSINESS FIT INTO CRITICAL INFRASTRUCTURE?

- **Small & Medium Businesses**
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Emergency Services
- Federal Government
- Healthcare and Public Health
- Nuclear
- Transportation Systems
- Water and Waste Water
- Financial

# FORMALIZED FRAMEWORKS AND RISK MANAGEMENT

- There are three things you can do about your risks:
  - Mitigate – fix the risks that you can fix
  - Transfer – buy insurance or utilize third party services (i.e. Cloud Services)
  - Accept – you can not have a solution for all risks.

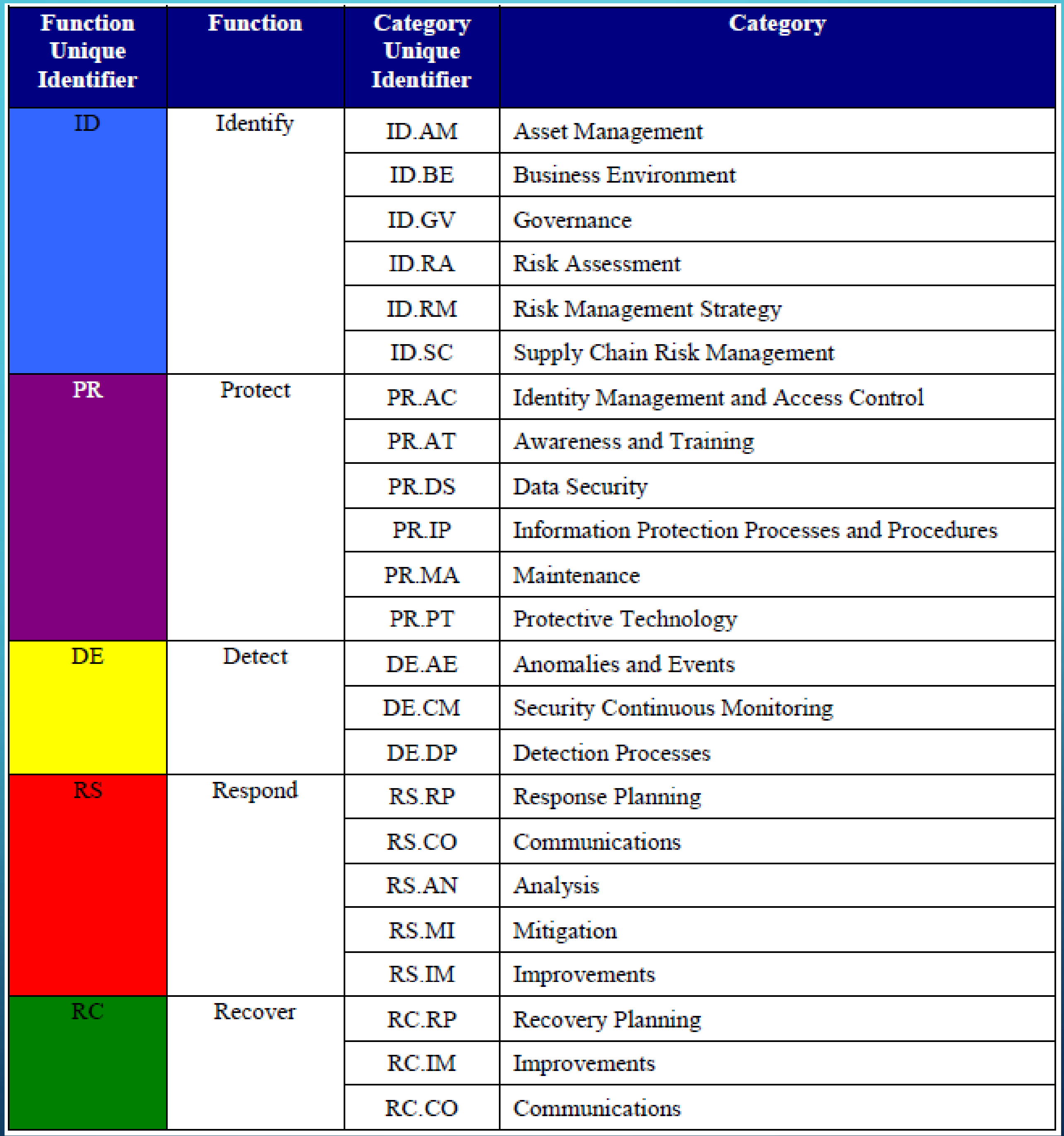
- You don't know what to do about risks until you identify them.
  - A formalized framework helps you identify and prioritize the risks.

# NIST CYBERSECURITY FRAMEWORK

- Developed by the National Institute of Standards and Technologies (NIST).
- Crosswalks to NIST 800-53, COBIT, ISO27001, etc., and uses key controls from each.
- Five functional cybersecurity areas.
- Twenty-three categories of protections.
- One-hundred-eight sub-categories (controls).
- Four Tiers of cybersecurity maturity.

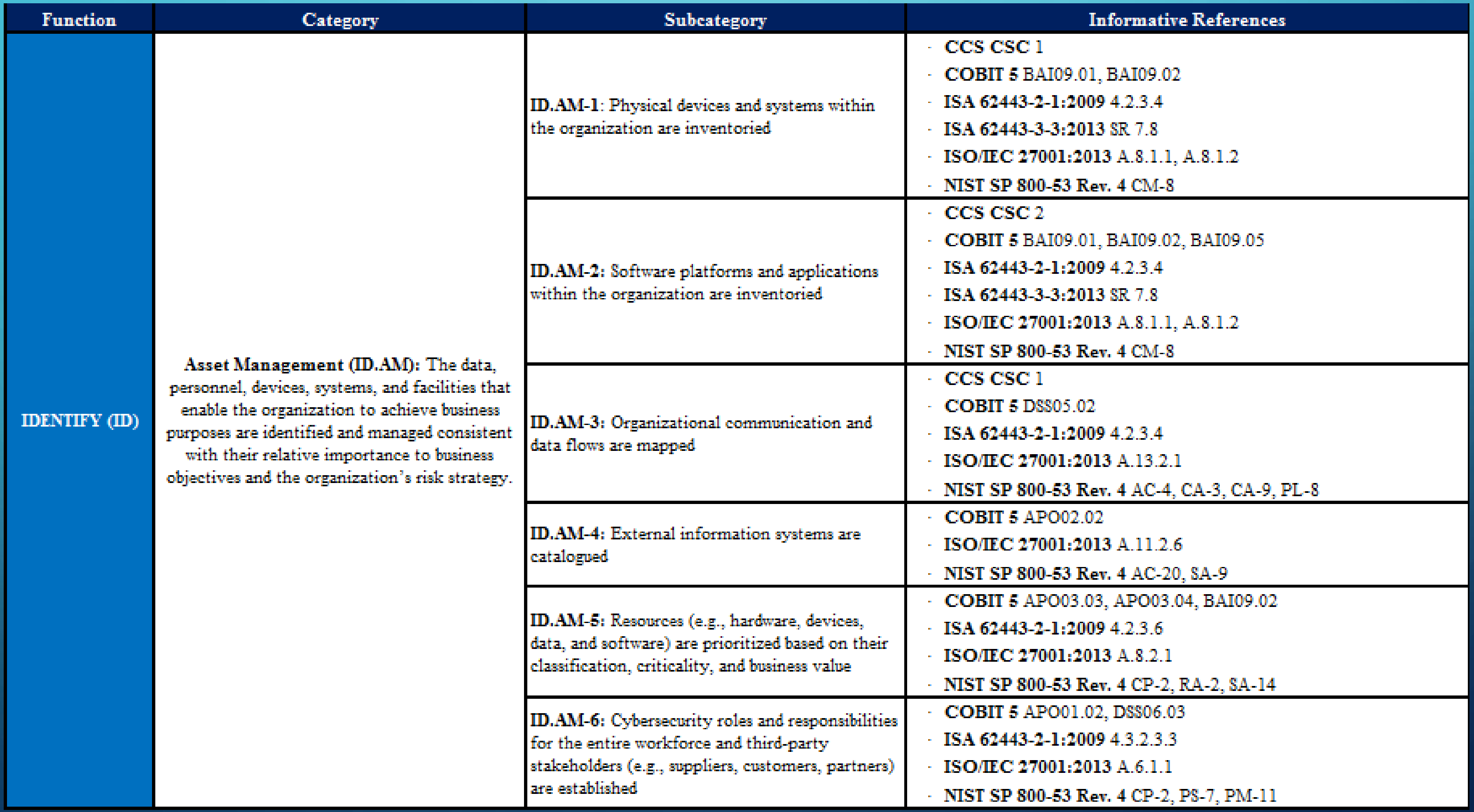
# CYBERSECURITY FRAMEWORK FUNCTION AREAS

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – 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.



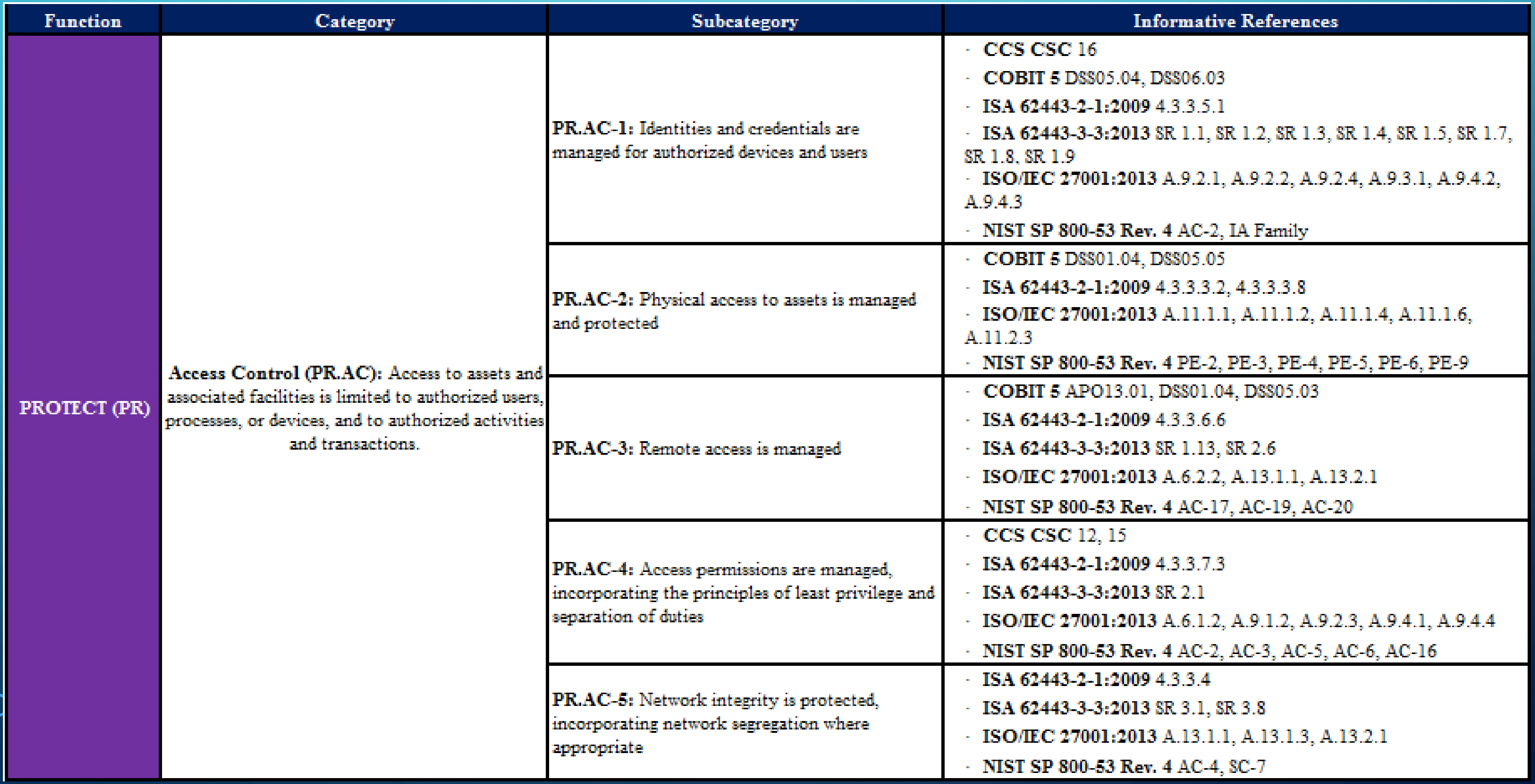
| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| | | ID.SC | Supply Chain Risk Management |
| PR | Protect | PR.AC | Identity Management and 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 |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

# NIST CSF EXAMPLE (IDENTIFY)



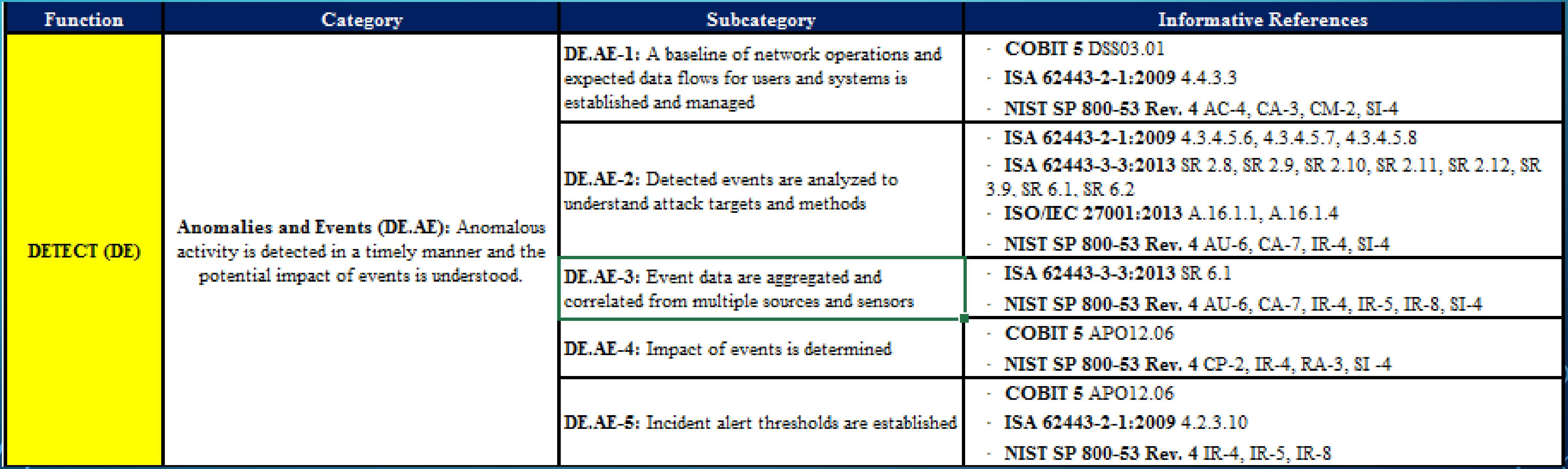
| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| IDENTIFY (ID) | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. | **ID.AM-1**: Physical devices and systems within the organization are inventoried | · **CCS CSC** 1<br>· **COBIT 5** BAI09.01, BAI09.02<br>· **ISA 62443-2-1:2009** 4.2.3.4<br>· **ISA 62443-3-3:2013** SR 7.8<br>· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2<br>· **NIST SP 800-53 Rev. 4** CM-8 |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | · **CCS CSC** 2<br>· **COBIT 5** BAI09.01, BAI09.02, BAI09.05<br>· **ISA 62443-2-1:2009** 4.2.3.4<br>· **ISA 62443-3-3:2013** SR 7.8<br>· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2<br>· **NIST SP 800-53 Rev. 4** CM-8 |
| | | **ID.AM-3:** Organizational communication and data flows are mapped | · **CCS CSC** 1<br>· **COBIT 5** DSS05.02<br>· **ISA 62443-2-1:2009** 4.2.3.4<br>· **ISO/IEC 27001:2013** A.13.2.1<br>· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8 |
| | | **ID.AM-4:** External information systems are catalogued | · **COBIT 5** APO02.02<br>· **ISO/IEC 27001:2013** A.11.2.6<br>· **NIST SP 800-53 Rev. 4** AC-20, SA-9 |
| | | **ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | · **COBIT 5** APO03.03, APO03.04, BAI09.02<br>· **ISA 62443-2-1:2009** 4.2.3.6<br>· **ISO/IEC 27001:2013** A.8.2.1<br>· **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14 |
| | | **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established | · **COBIT 5** APO01.02, DSS06.03<br>· **ISA 62443-2-1:2009** 4.3.2.3.3<br>· **ISO/IEC 27001:2013** A.6.1.1<br>· **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11 |

# NIST CSF EXAMPLE (PROTECT)



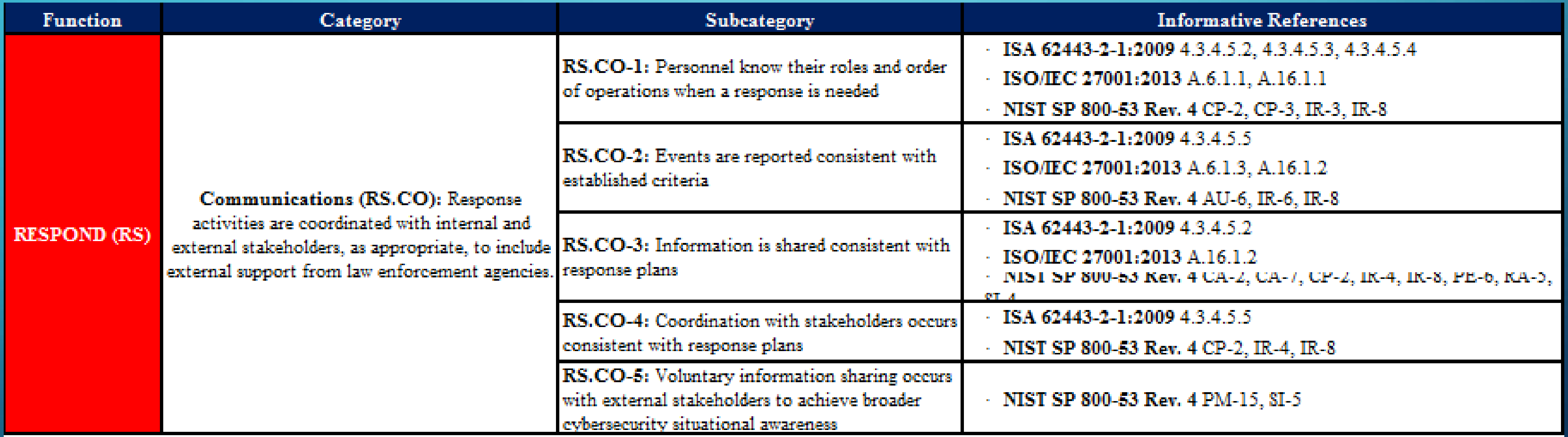
| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| **PROTECT (PR)** | **Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. | **PR.AC-1:** Identities and credentials are managed for authorized devices and users | · **CCS CSC** 16<br>· **COBIT 5** DSS05.04, DSS06.03<br>· **ISA 62443-2-1:2009** 4.3.3.5.1<br>· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9<br>· **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3<br>· **NIST SP 800-53 Rev. 4** AC-2, IA Family |
| | | **PR.AC-2:** Physical access to assets is managed and protected | · **COBIT 5** DSS01.04, DSS05.05<br>· **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8<br>· **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3<br>· **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 |
| | | **PR.AC-3:** Remote access is managed | · **COBIT 5** APO13.01, DSS01.04, DSS05.03<br>· **ISA 62443-2-1:2009** 4.3.3.6.6<br>· **ISA 62443-3-3:2013** SR 1.13, SR 2.6<br>· **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1<br>· **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20 |
| | | **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties | · **CCS CSC** 12, 15<br>· **ISA 62443-2-1:2009** 4.3.3.7.3<br>· **ISA 62443-3-3:2013** SR 2.1<br>· **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4<br>· **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16 |
| | | **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate | · **ISA 62443-2-1:2009** 4.3.3.4<br>· **ISA 62443-3-3:2013** SR 3.1, SR 3.8<br>· **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1<br>· **NIST SP 800-53 Rev. 4** AC-4, SC-7 |

# NIST CSF EXAMPLE (DETECT)



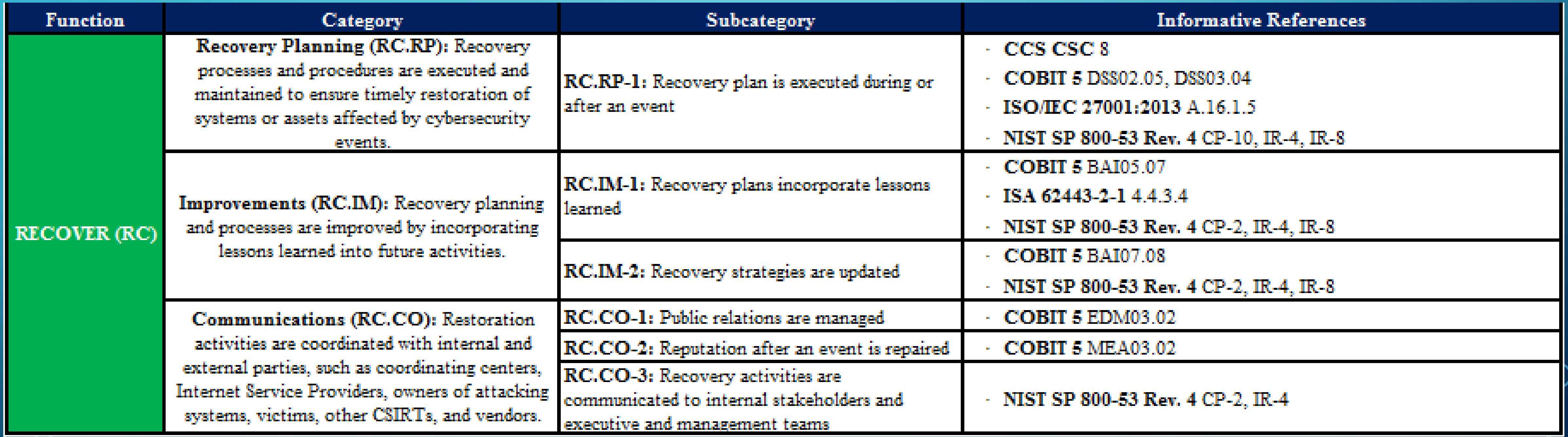
| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| **DETECT (DE)** | **Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood. | **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed | · **COBIT 5** DSS03.01<br>· **ISA 62443-2-1:2009** 4.4.3.3<br>· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4 |
| | | **DE.AE-2:** Detected events are analyzed to understand attack targets and methods | · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8<br>· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2<br>· **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4<br>· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4 |
| | | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | · **ISA 62443-3-3:2013** SR 6.1<br>· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 |
| | | **DE.AE-4:** Impact of events is determined | · **COBIT 5** APO12.06<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4 |
| | | **DE.AE-5:** Incident alert thresholds are established | · **COBIT 5** APO12.06<br>· **ISA 62443-2-1:2009** 4.2.3.10<br>· **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8 |

# NIST CSF EXAMPLE (RESPOND)



| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| **RESPOND (RS)** | **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | · **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4<br>· **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1<br>· **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8 |
| | | **RS.CO-2:** Events are reported consistent with established criteria | · **ISA 62443-2-1:2009** 4.3.4.5.5<br>· **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2<br>· **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8 |
| | | **RS.CO-3:** Information is shared consistent with response plans | · **ISA 62443-2-1:2009** 4.3.4.5.2<br>· **ISO/IEC 27001:2013** A.16.1.2<br>· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 |
| | | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans | · **ISA 62443-2-1:2009** 4.3.4.5.5<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 |
| | | **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | · **NIST SP 800-53 Rev. 4** PM-15, SI-5 |

# NIST CSF EXAMPLE (RECOVER)



| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| RECOVER (RC) | **Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events. | **RC.RP-1:** Recovery plan is executed during or after an event | · **CCS CSC** 8<br>· **COBIT 5** DSS02.05, DSS03.04<br>· **ISO/IEC 27001:2013** A.16.1.5<br>· **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8 |
| | **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | **RC.IM-1:** Recovery plans incorporate lessons learned | · **COBIT 5** BAI05.07<br>· **ISA 62443-2-1** 4.4.3.4<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 |
| | | **RC.IM-2:** Recovery strategies are updated | · **COBIT 5** BAI07.08<br>· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8 |
| | **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. | **RC.CO-1:** Public relations are managed | · **COBIT 5** EDM03.02 |
| | | **RC.CO-2:** Reputation after an event is repaired | · **COBIT 5** MEA03.02 |
| | | **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams | · **NIST SP 800-53 Rev. 4** CP-2, IR-4 |

# CYBERSECURITY MATURITY TIERS

- Four tiers of maturity.
- Describe where the organization is with respect to the ability to secure their IT environment.
- The goal is to thoughtfully, purposefully, and deliberately achieve Tier 4: Adaptive maturity.
- Maturity assessments need to be on-going.

# TIER 1: PARTIAL

- ***Risk Management Process*** – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- ***Integrated Risk Management Program*** – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.
- ***External Participation*** – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

# TIER 2: RISK INFORMED

- ***Risk Management Process*** – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- ***Integrated Risk Management Program*** – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
- ***External Participation*** – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.

# TIER 3: REPEATABLE

- ***Risk Management Process*** – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- ***Integrated Risk Management Program*** – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.
- ***External Participation*** - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

# TIER 4: ADAPTIVE

- ***Risk Management Process*** – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving, sophisticated threats.

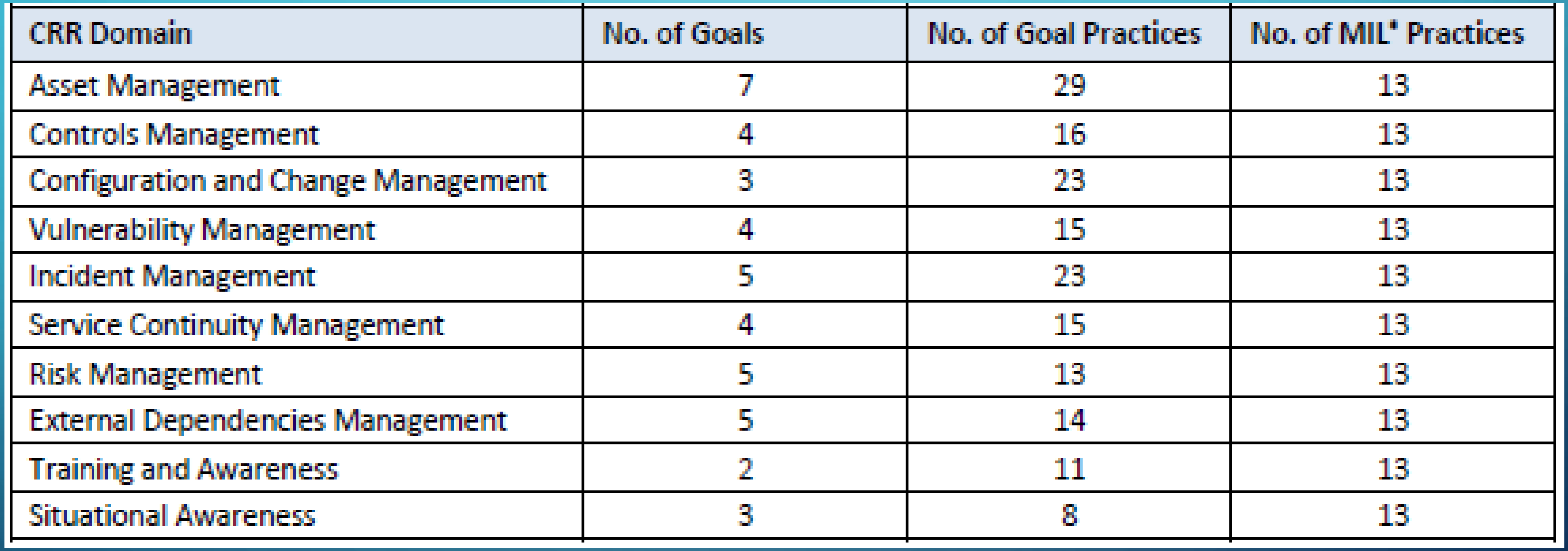
- ***Integrated Risk Management Program*** – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.

- ***External Participation*** - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

# CYBER RESILIENCE REVIEW

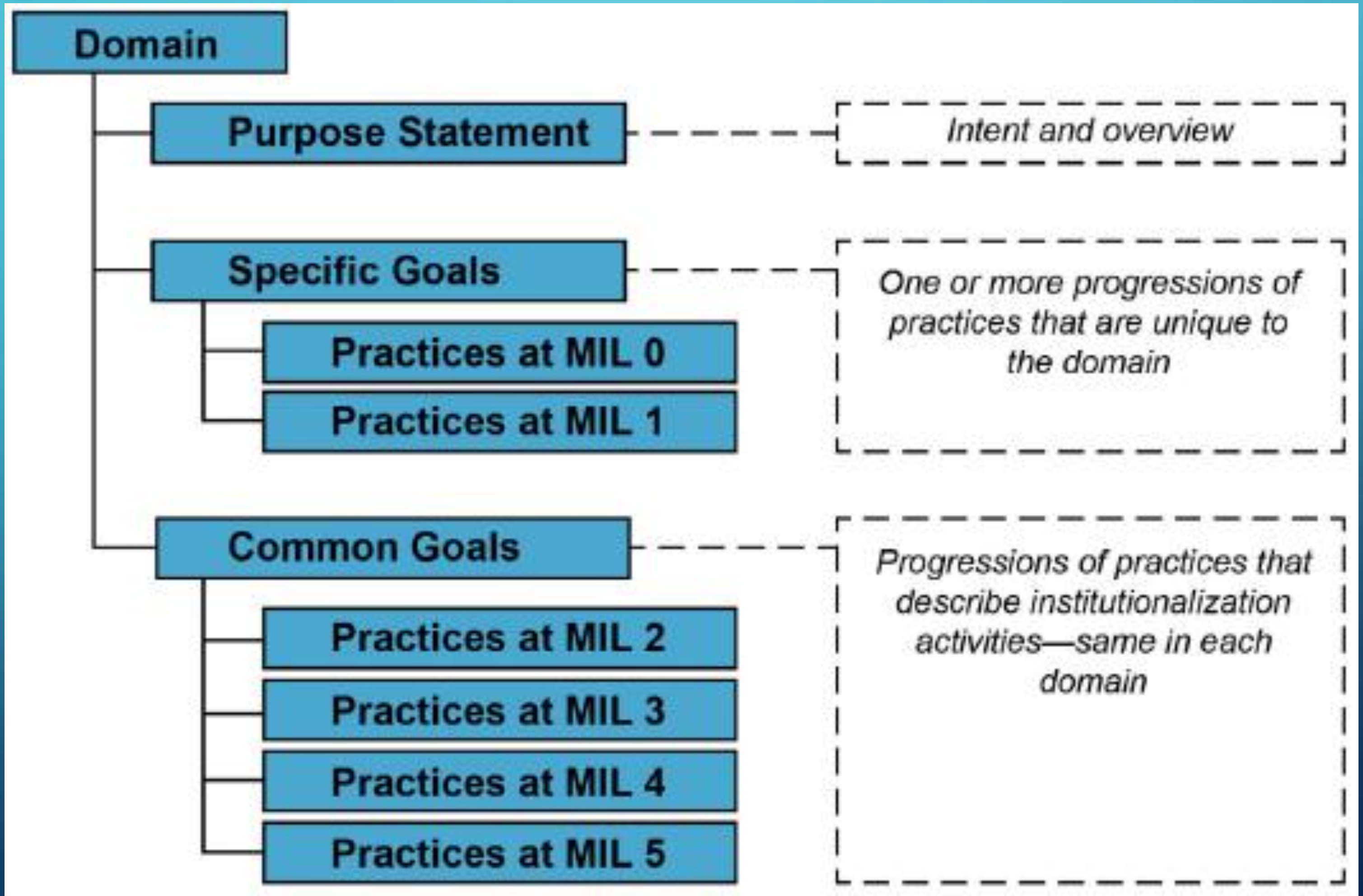
- Developed by DHS Office of Cybersecurity and Communications.
- Closely aligns with NIST Cybersecurity Framework
- No-cost, Voluntary, non-technical assessment.
- Can be done as a self-assessment.
- Ten domains, Six Maturity Indicator Levels (MIL)

# CRR DOMAIN COMPOSITION



| CRR Domain | No. of Goals | No. of Goal Practices | No. of MIL* Practices |
|---|---|---|---|
| Asset Management | 7 | 29 | 13 |
| Controls Management | 4 | 16 | 13 |
| Configuration and Change Management | 3 | 23 | 13 |
| Vulnerability Management | 4 | 15 | 13 |
| Incident Management | 5 | 23 | 13 |
| Service Continuity Management | 4 | 15 | 13 |
| Risk Management | 5 | 13 | 13 |
| External Dependencies Management | 5 | 14 | 13 |
| Training and Awareness | 2 | 11 | 13 |
| Situational Awareness | 3 | 8 | 13 |

# CRR DOMAIN ARCHITECTURE



Domain

- Purpose Statement — *Intent and overview*
- Specific Goals — *One or more progressions of practices that are unique to the domain*
  - Practices at MIL 0
  - Practices at MIL 1
- Common Goals — *Progressions of practices that describe institutionalization activities—same in each domain*
  - Practices at MIL 2
  - Practices at MIL 3
  - Practices at MIL 4
  - Practices at MIL 5

# CRR MATURITY INDICATOR LEVELS (MIL)

- **<u>MIL 0 Incomplete</u>** - Practices in the domain are not being performed as measured by responses to the relevant CRR questions in the domain.

- **<u>MIL 1 Performed</u>** - All practices that support the goals in a domain are being performed as measured by responses to the relevant CRR questions.

- **<u>MIL 2 Planned</u>** - A specific practice in the CRR domain is not only performed but is also supported by planning, stakeholders, and relevant standards and guidelines.

# CRR MATURITY INDICATOR LEVELS (MIL)

- **MIL 3 Managed** - All practices in a domain are performed, planned, and have the basic governance infrastructure in place to support the process.
- **MIL 4 Measured** - All practices in a domain are performed, planned, managed, monitored, and controlled.
- **MIL 5 Defined** - All practices in a domain are performed, planned, managed, measured, and consistent across all constituencies within an organization who have a vested interest in the performance of the practice.

# WRAPPING IT ALL UP

- Certain small businesses can be considered part of the Critical Infrastructure.
- Every small business should consider cybersecurity a top priority.
- There are a number of free and low-cost solutions to help you assess your security posture.
- Formalized frameworks help you implement and maintain a consistent cybersecurity program.
  - Cybersecurity Framework
  - Cyber Resilience Review
- The goal is to purposefully and deliberately strive to attain high levels of cybersecurity program maturity.

# WHAT YOU CAN DO

- Even if you choose not to implement one of these formalized frameworks, at the very least, you should:
  - **Risk Management** – Know your environment, know what your risks are, and know what you can do to mitigate, transfer, or accept the risks.
  - **Employee Training** – Ensure that your employees know how to keep your assets and data safe, especially while connected to the Internet.
  - **Rules of Behavior** – Have formal policies governing acceptable use of company owned computing assets, and make your employees sign them
  - **Inventories** - know what hardware and software you have on your network.
  - **Access Control** – know who is connected to your network, and what they are allowed to do.
  - **Vulnerability Management** – know what vulnerabilities are on your network and get them fixed.
  - **Business Continuity** – Have a plan to be able to protect data and recover if a disaster or some other emergency strikes.

# REFERENCES AND RESOURCES

- Small Business, Big Threat
  - https://smallbusinessbigthreat.com/
- Internet Security Essentials for Business 2.0
  - https://www.uschamber.com/CybersecurityEssentials
- NIST: Cybersecurity Framework
  - https://www.us-cert.gov/ccubedvp/cybersecurity-framework
- US-CERT: Critical Infrastructure Cyber Community Voluntary Program
  - https://www.us-cert.gov/ccubedvp

# REFERENCES AND RESOURCES

- US-CERT: Resources for Small and Midsize Businesses
  - https://www.us-cert.gov/ccubedvp/smb
- ICS-CERT: Training Available Through ICS-CERT
  - https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT
- Colorado Governor’s Office of Information technology, Office of Information Security (OIS)
  - http://www.oit.state.co.us/ois
- Article: “President Signs Cybersecurity Act Into Law”
  - https://www.scmagazine.com/president-signs-nist-small-business-cybersecurity-act-into-law/article/789147/?utm_source=newsletter&utm_medium=email&utm_campaign=SCUS_Newswire_20180820&email_hash=3b55642160677fb4bdff433c5f488d04&hmSubId=tTWs893tySM1

Q&A