Guide to Cybersecurity Framework – Become Cyber Resilient

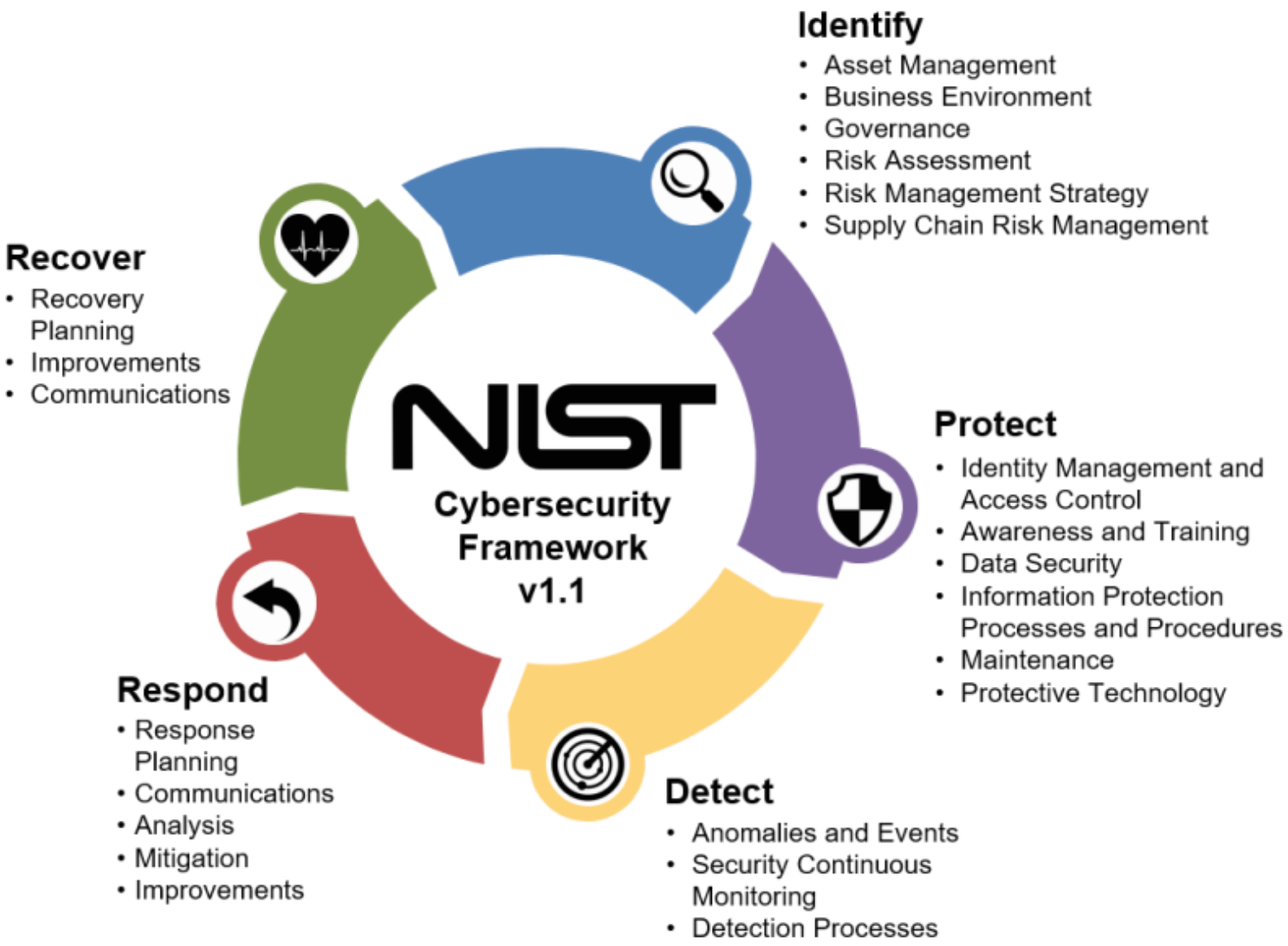
Cybersecurity is a living process which demands continuous efforts to improve upon our own weaknesses

Key Requirements to build a successful cybersecurity program

- Discipline
- Attention to details
- Zero Complacency
- Proactive Communication
- Choosing the Right Framework

Approach Methodology

Cybersecurity Services – Based on NIST 1.1 Framework


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 and 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 v1.1

Identify

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

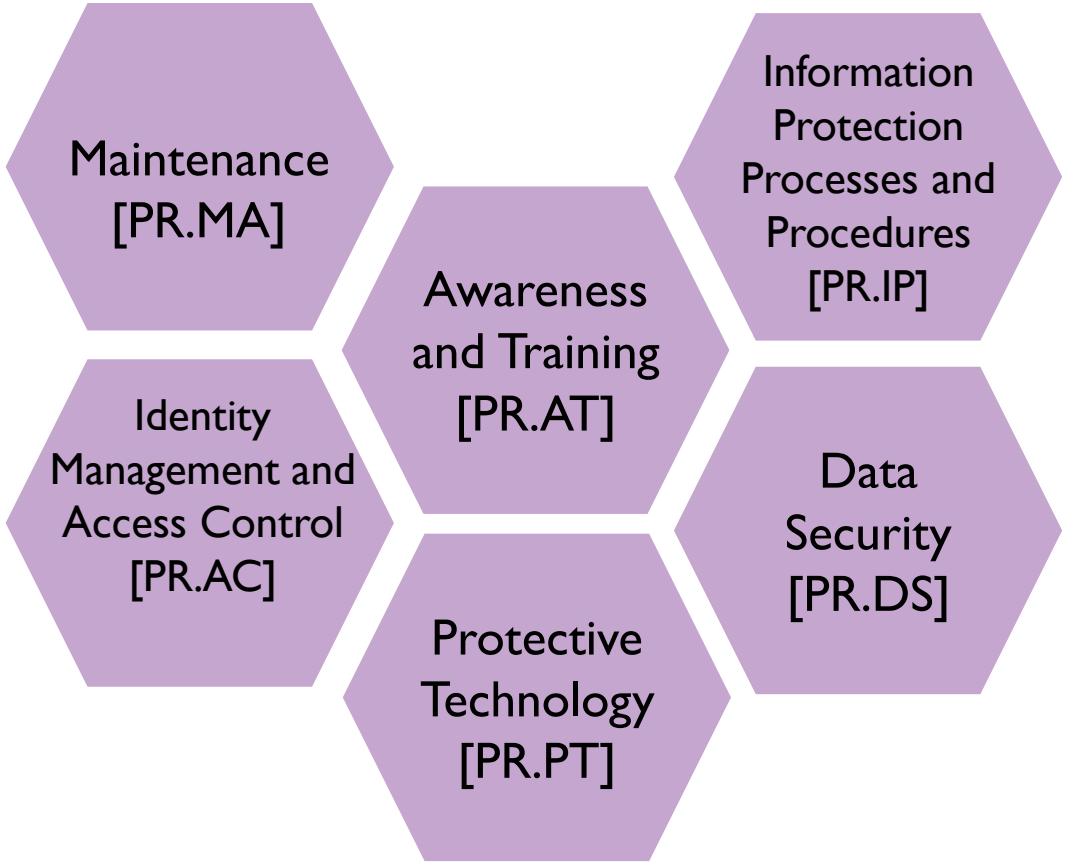
Identify Activities

- Identify critical business processes
- Document Information flows
- Establish policies for cybersecurity that includes roles and responsibilities
- Maintain hardware and software inventory
- Identify contracts with external partners
- Identify Risk Management processes

Protect

Develop and implement the appropriate safeguards to ensure delivery of services.

Protect Activities



- **Manage access to assets and information**
- **Conduct regular backups**
- **Protect sensitive data**
- **Patch operating systems and applications**
- **Create response and recovery plans**
- **Protect your network**
- **Train your employees**

Detect

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

Detect Activities

Anomalies and Events [DE.AE]

Continuous Monitoring [DE.CM]

- Install and update anti-virus and other malware detection software
- Know what are expected data flows for your business
- Maintain and monitor logs

Respond Pillar

Response Planning [RS.RP]

Communications [RS.CO]

- Coordinate with internal and external stakeholders
- Ensure response plans are tested
- Ensure response plans are updated

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.

Recover Activities

Recovery Planning [RC.RP]

Communications [RC.CO]

- Manage public relations and company reputation
- Communicate with internal and external stakeholders
- Ensure recovery plans are updated
- Consider cyber insurance

Accelerating your Cyber Resilience Program

OUR TECHNOLOGY EXPERTISE

IDENTITY AND ACCESS MANAGEMENT

- Adaptive Identity Governance
- Adaptive Access Management
- Adaptive Privilege User

GOVERNANCE RISK AND COMPLIANCE

- eDiscovery & Classification
- Information Management

END POINT SECURITY

- Lifecycle management
- Patching & containerization
- Application virtualization
- Mobile and Server Management

SECURITY OPERATIONS

- Real-time detection
- Workflow automation
- Open source data ingestion
- Hunt and investigation

DATA SECURITY

- Data De-identification (encryption/tokenization)
- Key management
- H/W-based trust assurance
- Messaging security

APP SECURITY

- Static, Dynamic, & Runtime
- application testing
- Application security-as-a-service
- Dev-sec-ops