# NIST Cybersecurity Framework Core

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

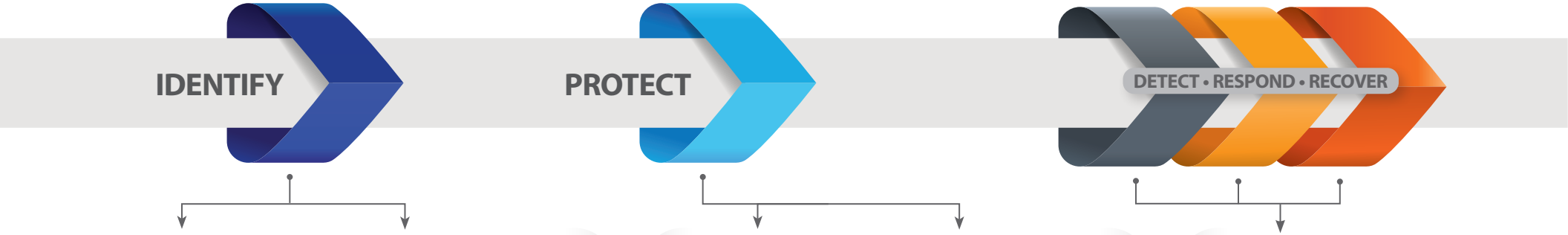
- Identity Management & Access Control
- Awareness and Training
- Data Security
- Information Protection Process & Procedures
- Maintenance
- ProtectiveTechnology

- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

- Recover Planning
- Improvements
- Communications

# FitNetworks Approach




### Leadership & Commitment
- Business Leaders develop policies to guide NIST framework implementation
  - Management of change
  - Risk assessment
  - Other

### Deliverables:
- Cybersecurity management of change policy & procedures
- Cybersecurity risk assessment policy & procedures

### Assess & Profile
- NIST framework assessment
- Strategic/high level risk assessment
  - Across entire business
  - A single facility

### Deliverables:
- NIST framework assessment for current process/practices
- Profile determination and report documenting rational
- Risk assessment report

### Monitoring
- Real time monitoring
  - SIEM
  - Network Auditing SW
- Develop target profile
- Develop and analyze gaps

### Deliverables:
- Detailed monitoring report with analysis of results
- Face-to-face meeting with interpretation and clarification of monitoring report and findings
- Action plan for gaps

### Implementation
- Implement Gap Closure Plan
- Detailed Risk Assessments
  - Systems
  - Platforms
- Implement Network-based security tools
- If DHS CFATS applies then isolate Process Control Network
- Develop DMZ implementation plan
- Standup DMZ

### Ongoing
- Detect
  - Tools
  - Systems
- Respond
  - Procedures
  - Processes
  - Resources
- Recover
  - Plans
  - Resources

FITNETWORKS

© FitNetworks 2019 | info@fitnetworks.com | fitnetworks.com