SKYLINE TECHNOLOGYSOLUTIONS

The Why, What, and How of

Cybersecurity

Introductions

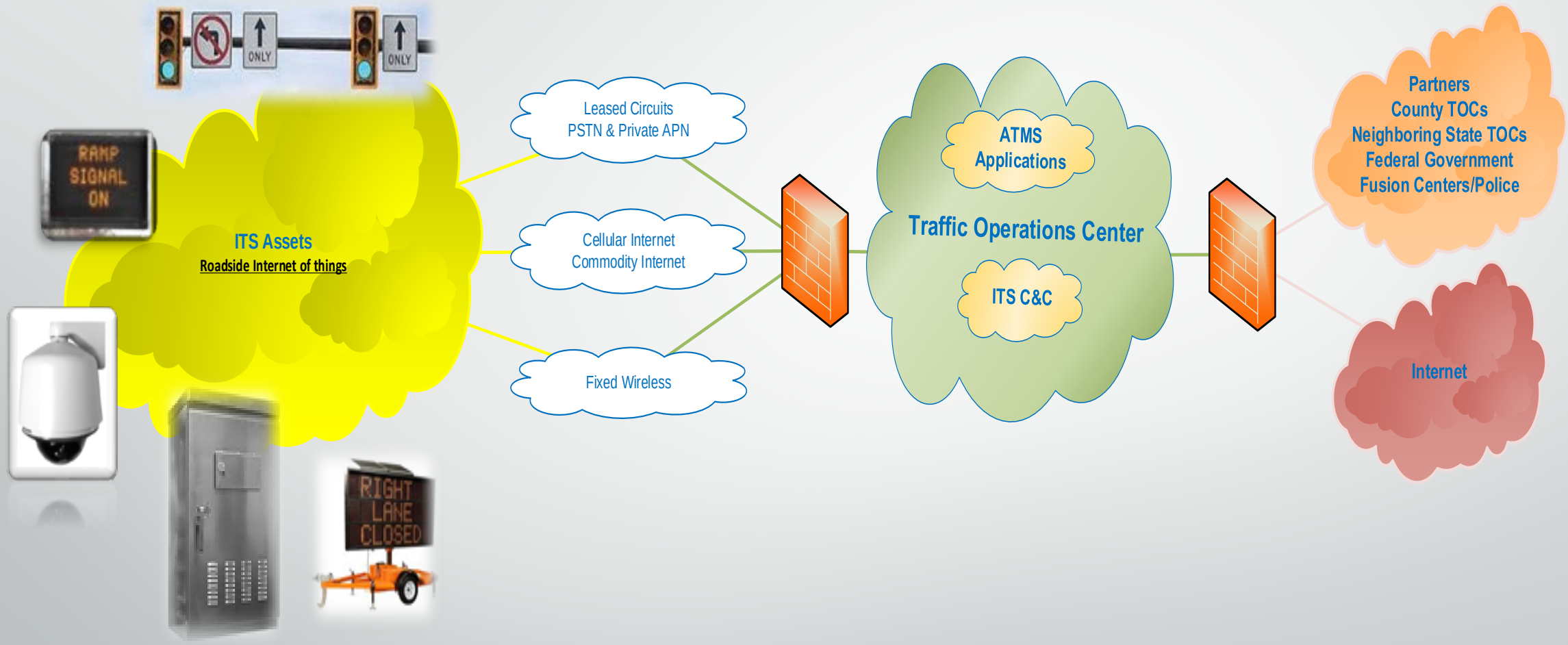
- **Skyline Technology Solutions**
  - **Tom Burgoon - BD ITS Practice**
  - **Laura Gomez-Martin – Cybersecurity Compliance Advisor**
  - **Chip Stewart – Principal Consultant**
- **Mission Secure**
  - **Rick Tiene – VP, Government and Critical Infrastructure**


1st the
WHY


2nd the
WHAT


3rd the
HOW

DOT Networks



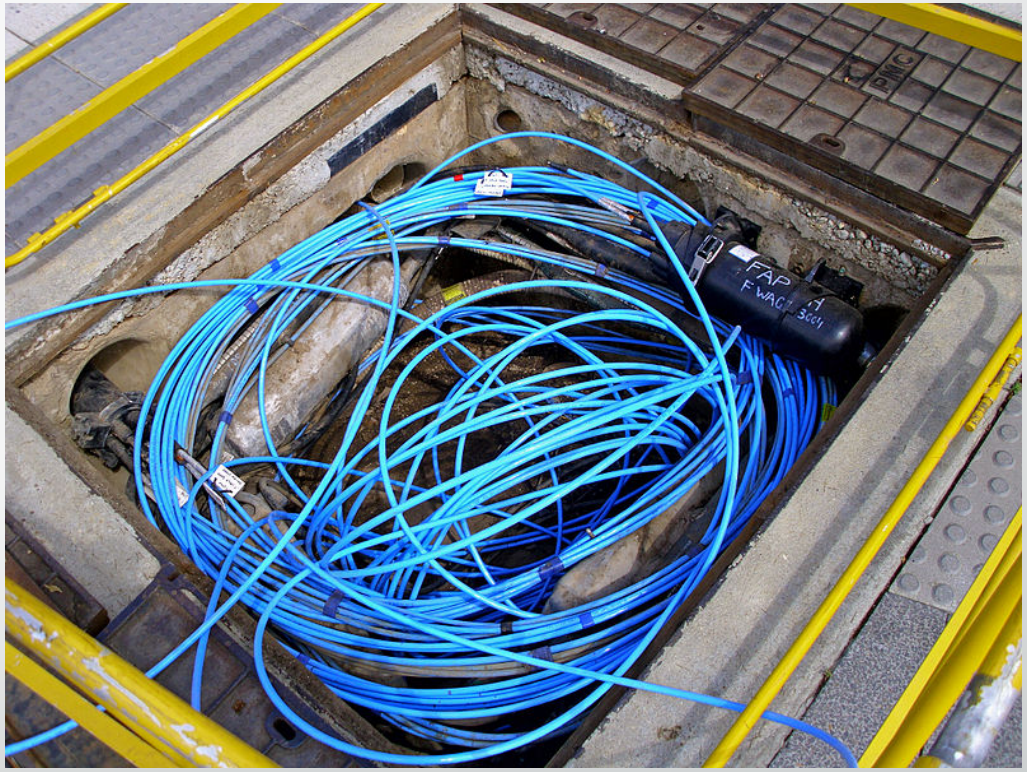
Road Side Devices → Field Network → Trusted Network → External Networks

Cybersecurity Quick Primer

Road Side Devices

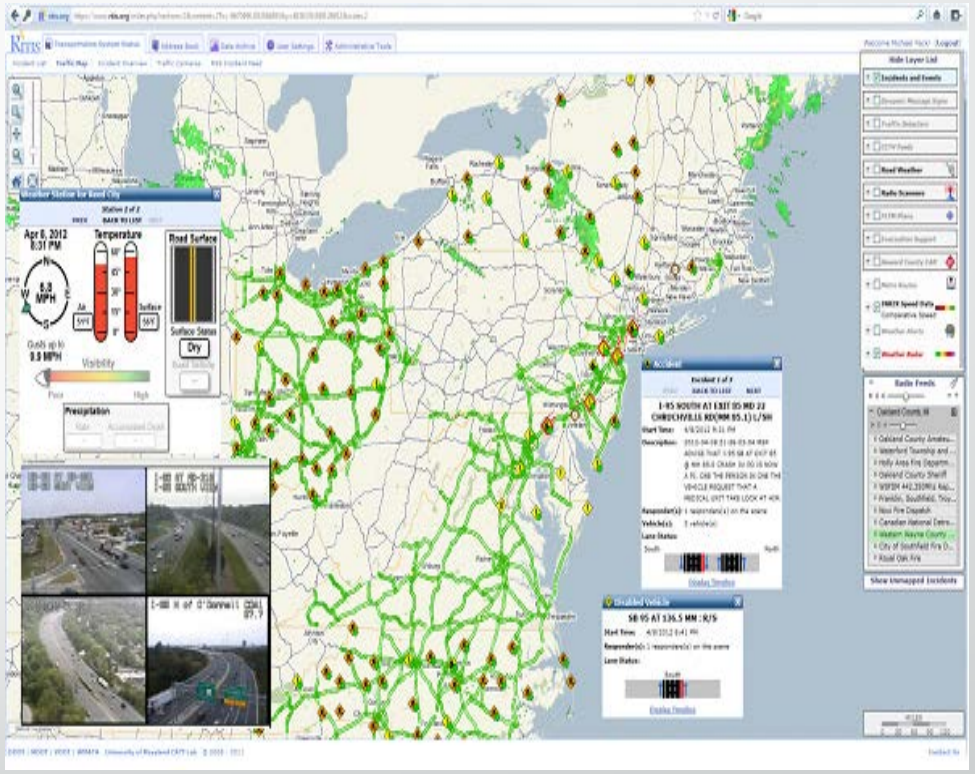
Road Side Devices → Field Network → Trusted Network → External Networks

Field Network



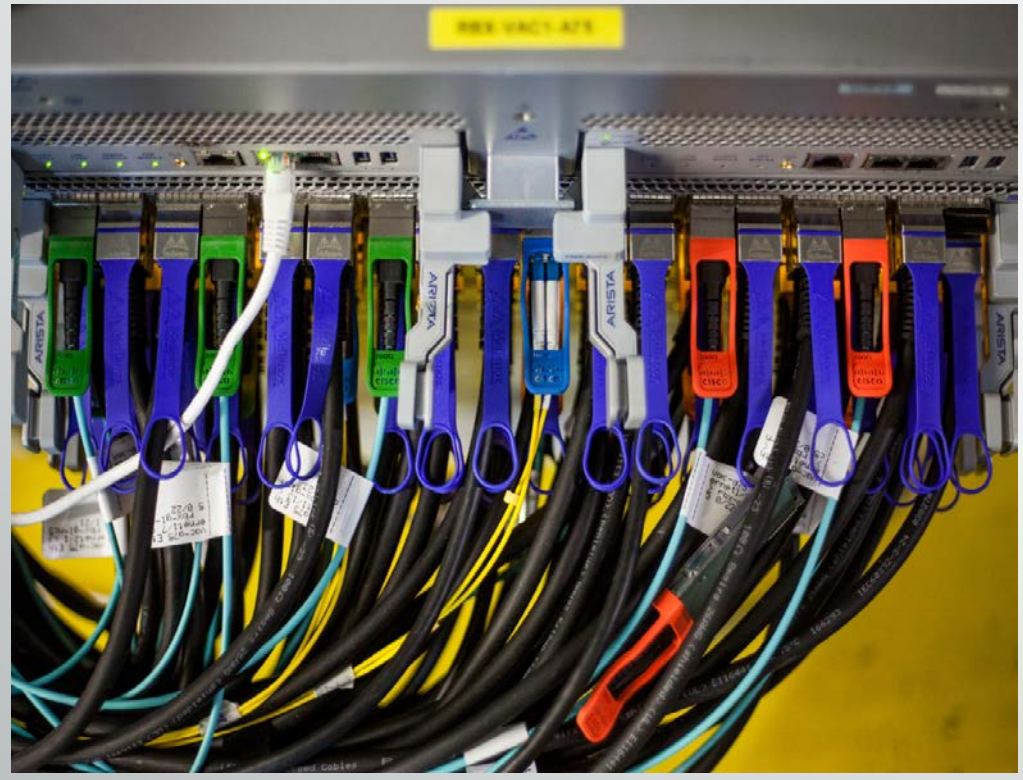
Road Side Devices → **Field Network** → Trusted Network → External Networks

Trusted Network



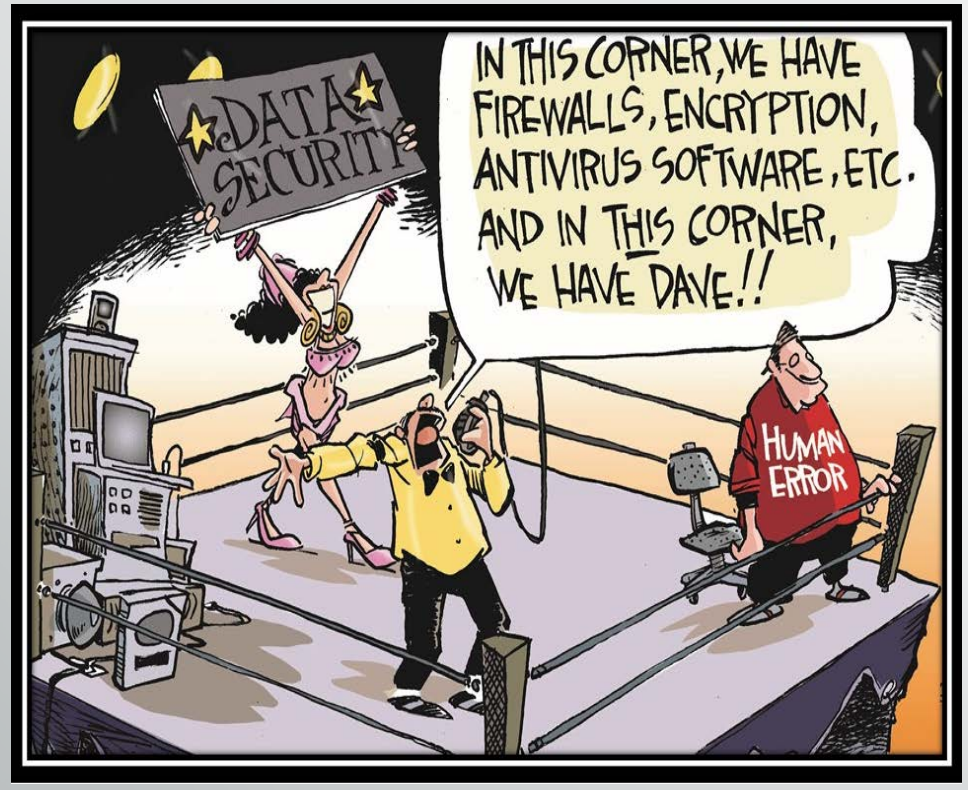
Road Side Devices → Field Network → **Trusted Network** → External Networks

External Networks



Road Side Devices → Field Network → Trusted Network → External Networks

Insider Threats



Road Side Devices → Field Network → Trusted Network → External Networks

Security is simple – not easy

What is Cybersecurity

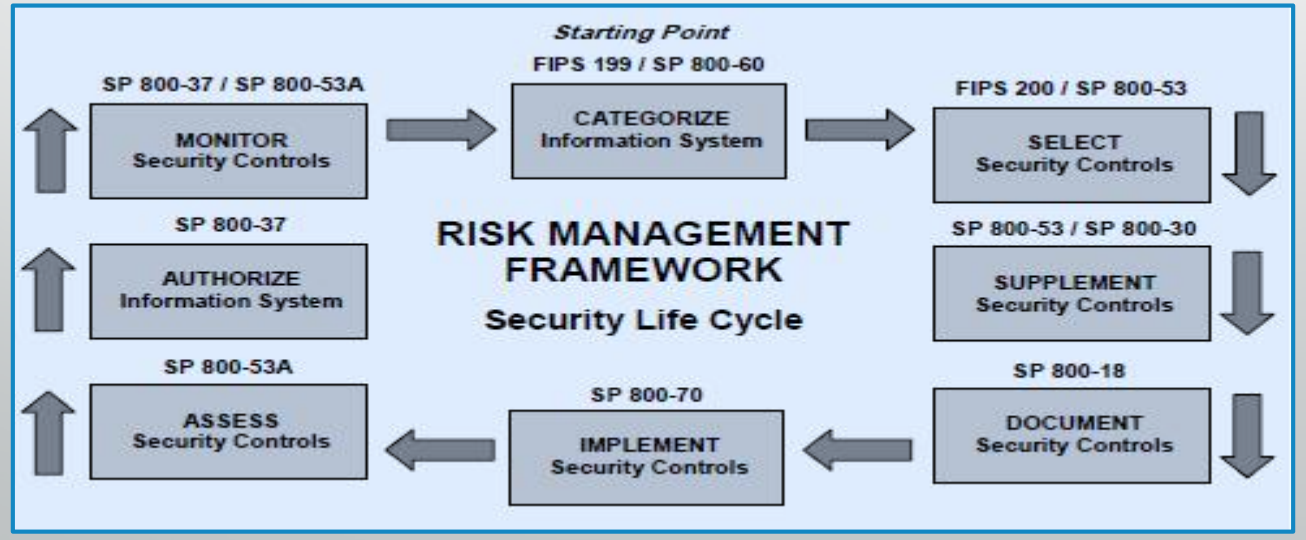
- Policy
- Detailed Controls and Configurations
- Continuous Monitoring
- Incident Response

What Cybersecurity is Not

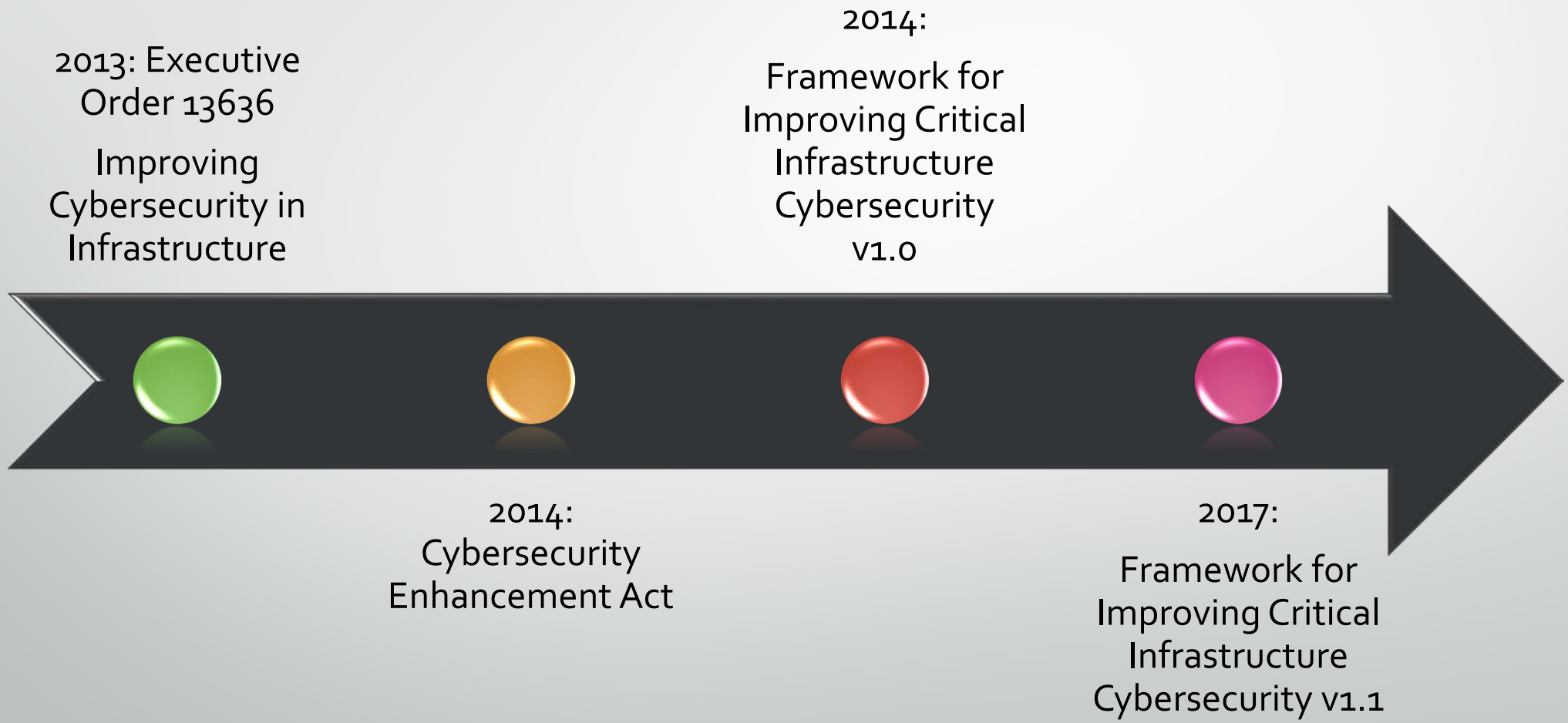
- Total Elimination of Risk
- One Tool Solution
- A Traditional IT Function

Informative Resources

- CIS Top 20
- ISO 27001
- NIST SP 800-53R4



Recent Critical Infrastructure Developments

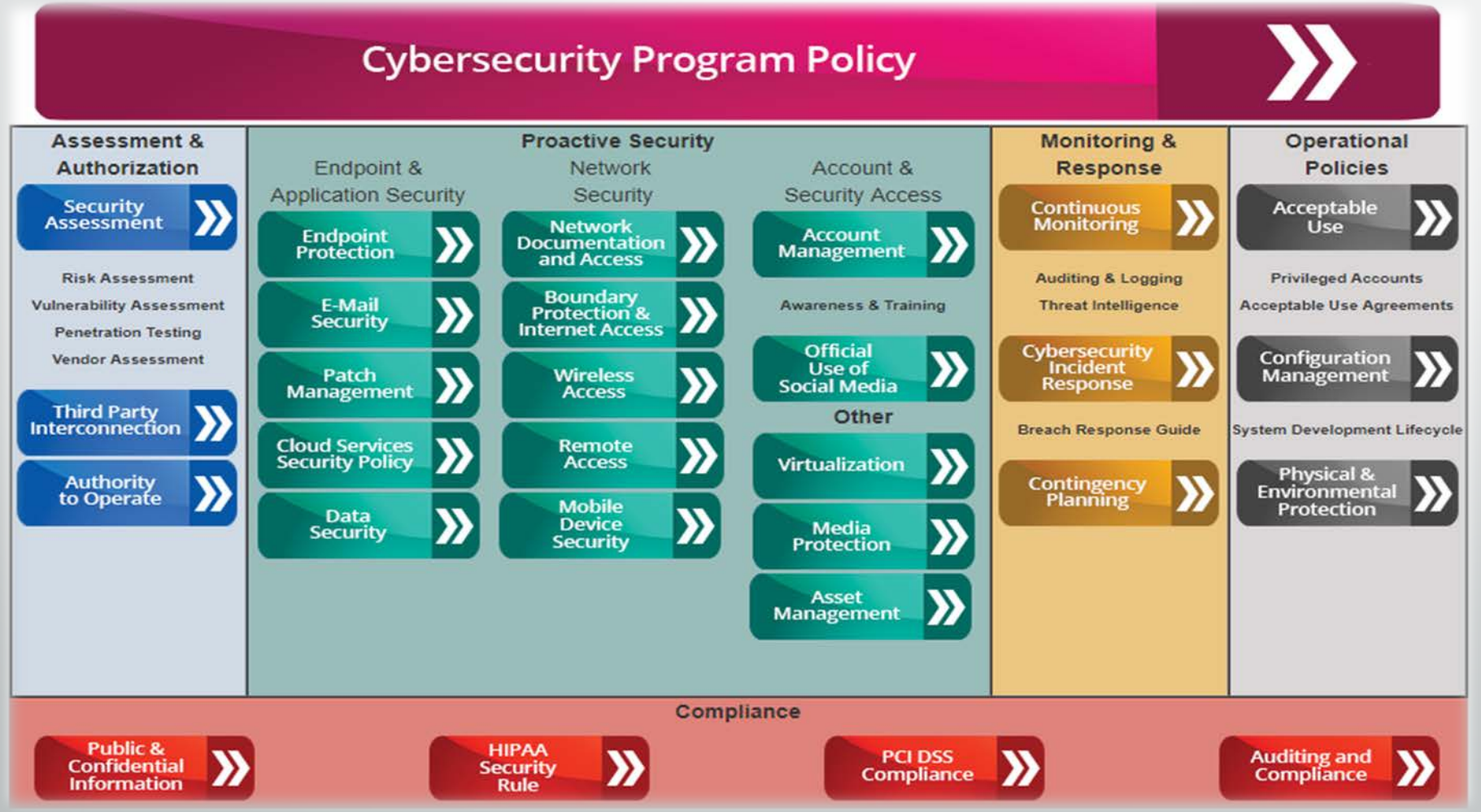


Framework for Improving Critical Infrastructure Cybersecurity

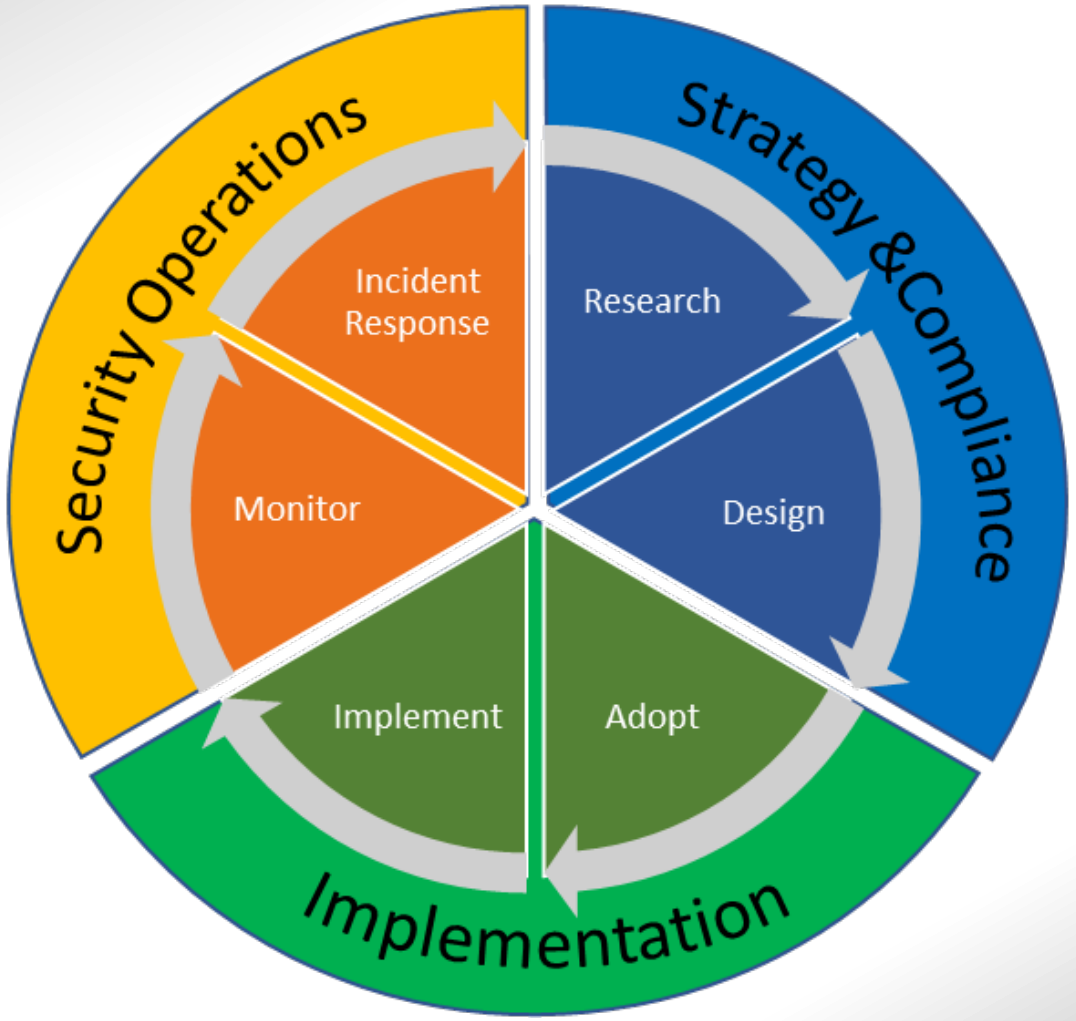
Function	Category	Subcategory	Informative References
IDENTIFY	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **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 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **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 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1 • **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

Department of INFORMATION TECHNOLOGY

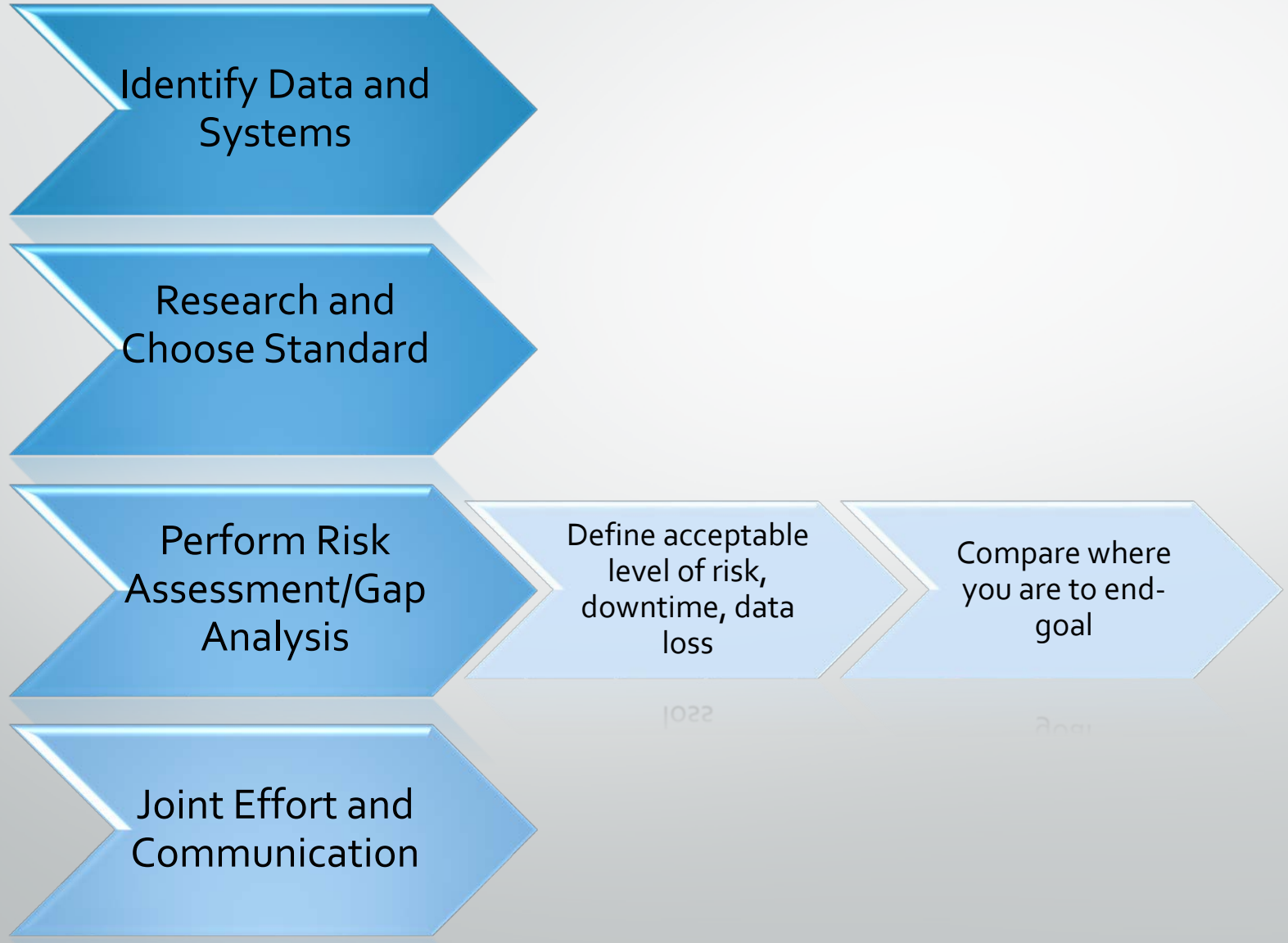
Cybersecurity Program for Maryland DoIT



Cybersecurity Program

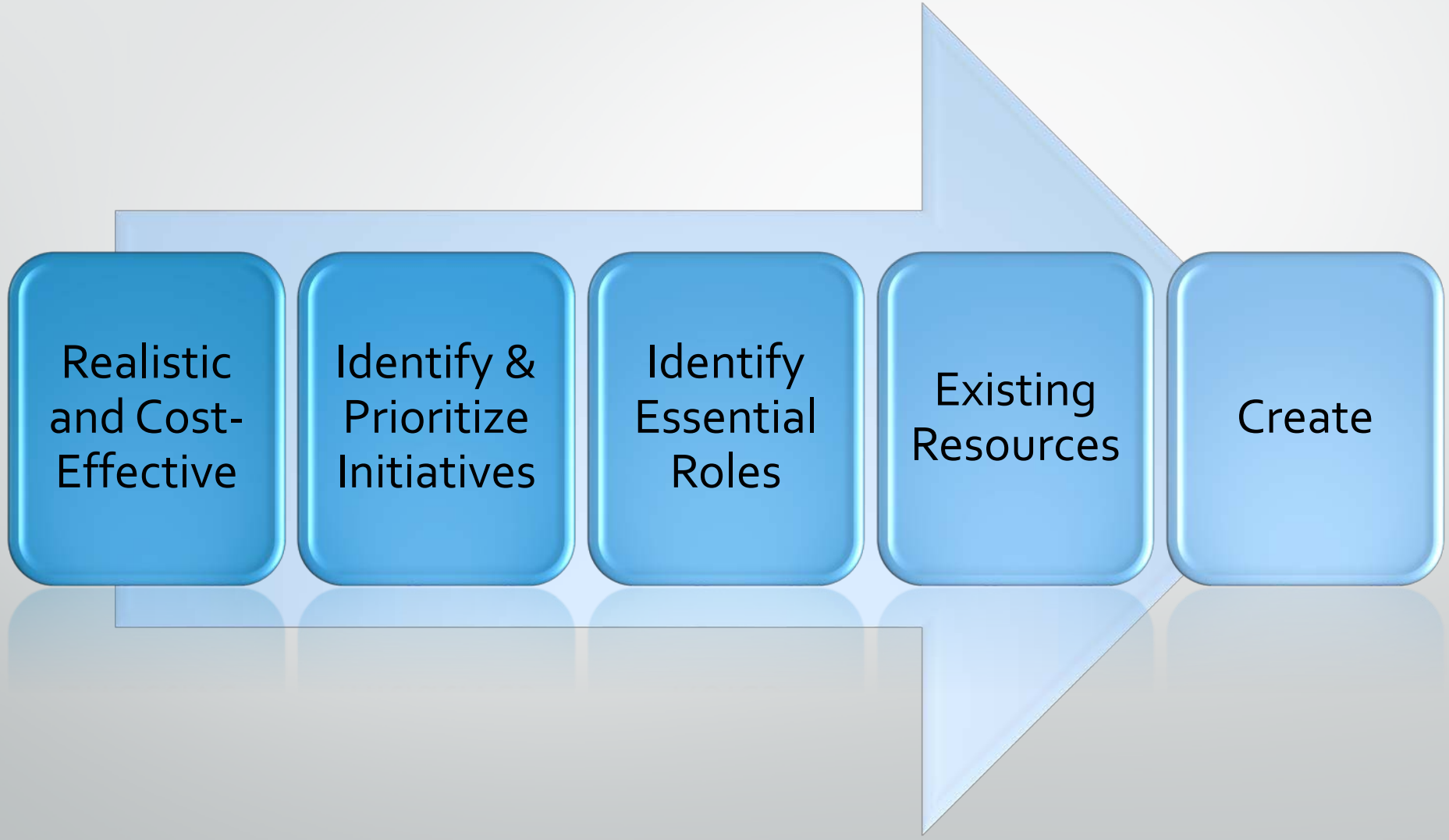


Research



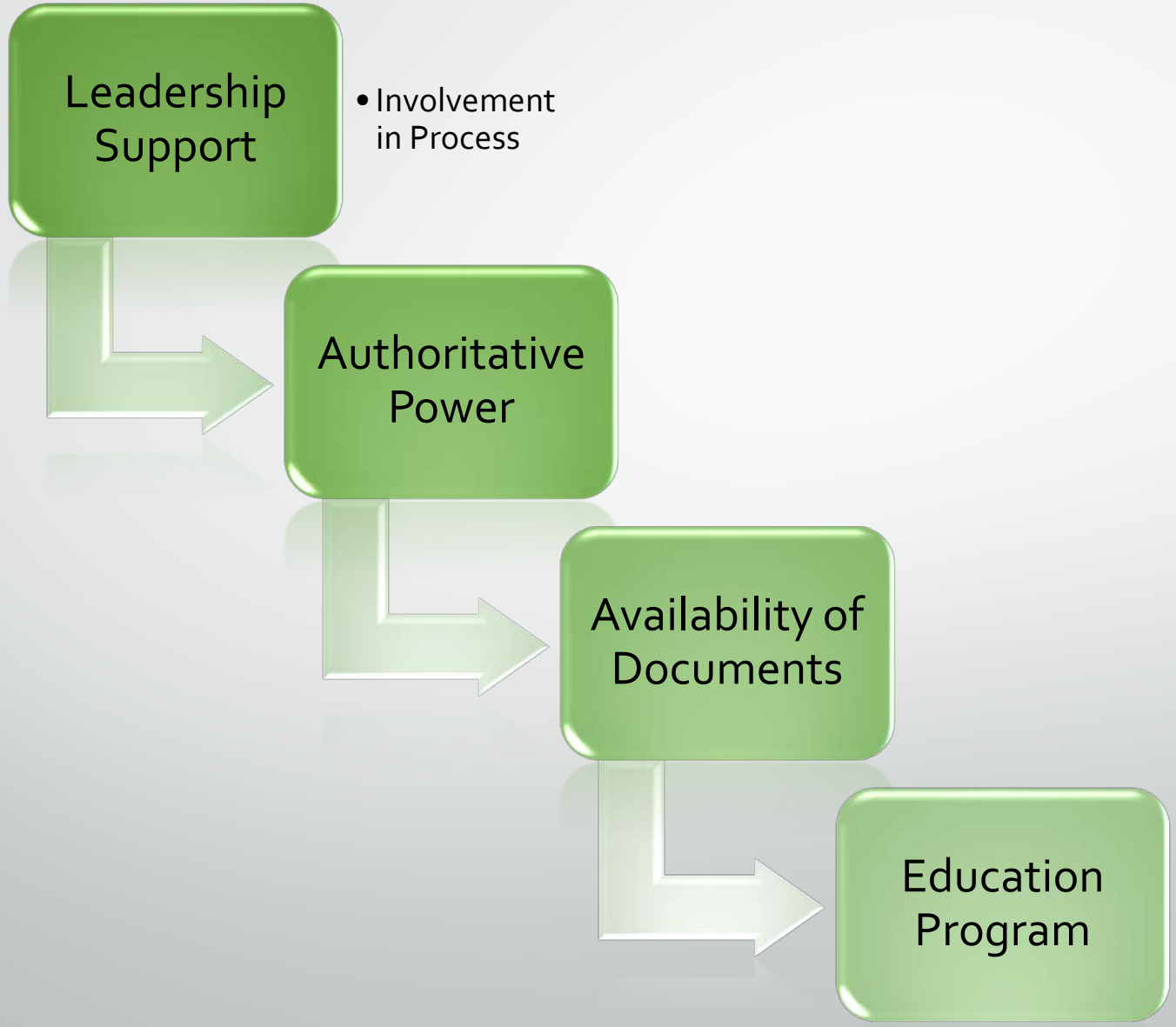
SKYLINE TECHNOLOGY SOLUTIONS

Design

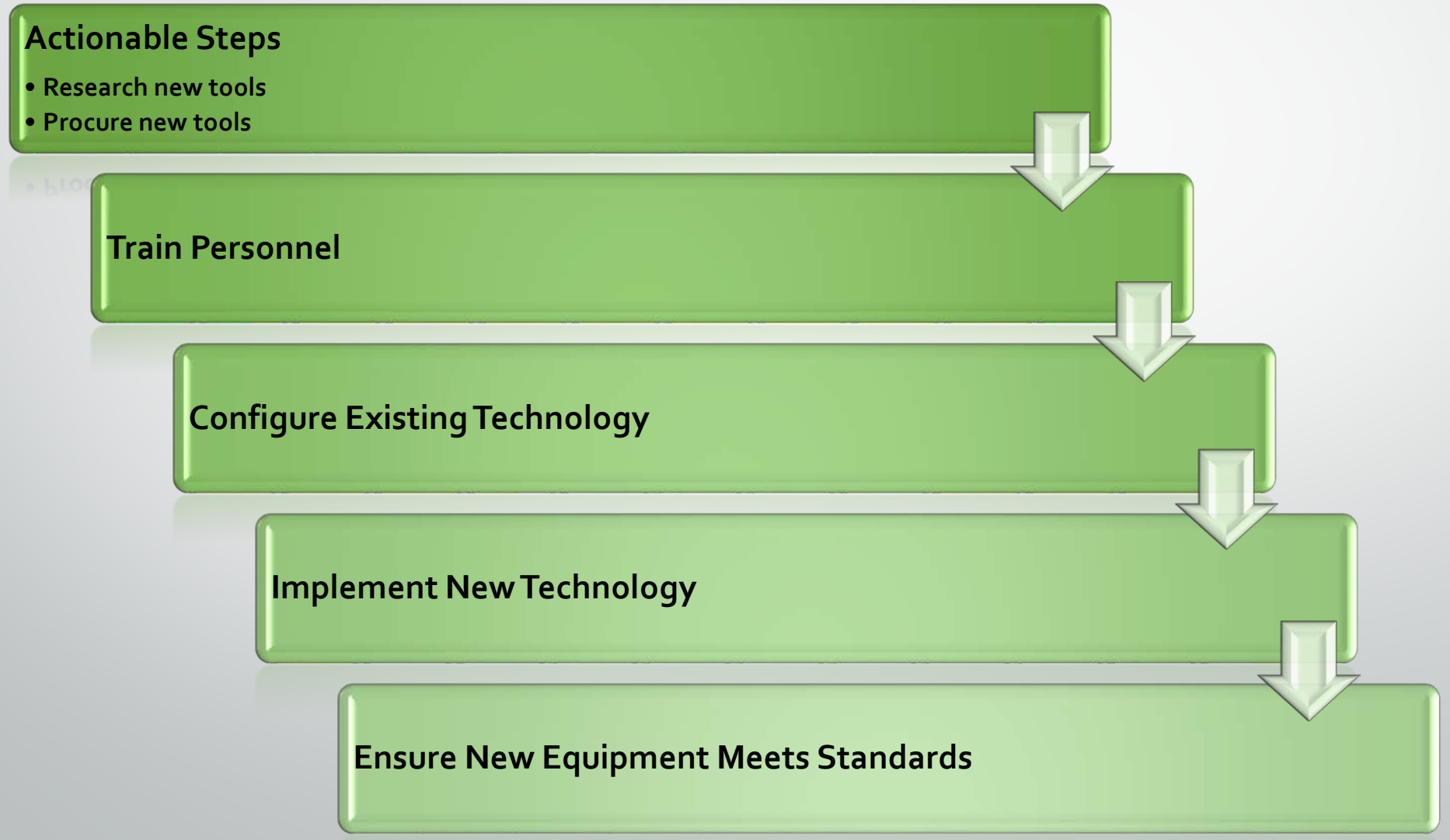


SKYLINE TECHNOLOGY SOLUTIONS

Adopt


Leadership Support
• Involvement in Process
Authoritative Power
Availability of Documents
Education Program

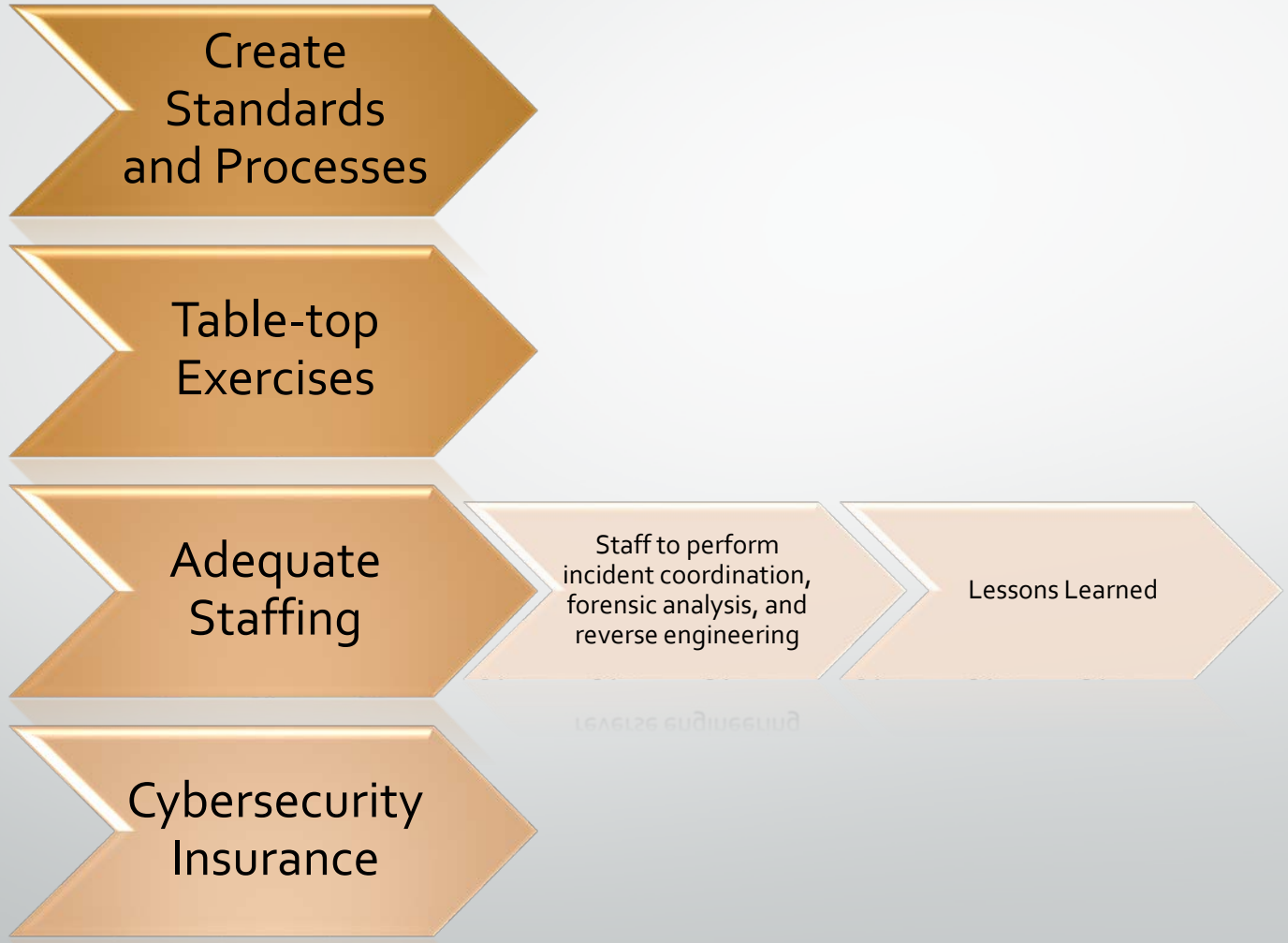
Implementation



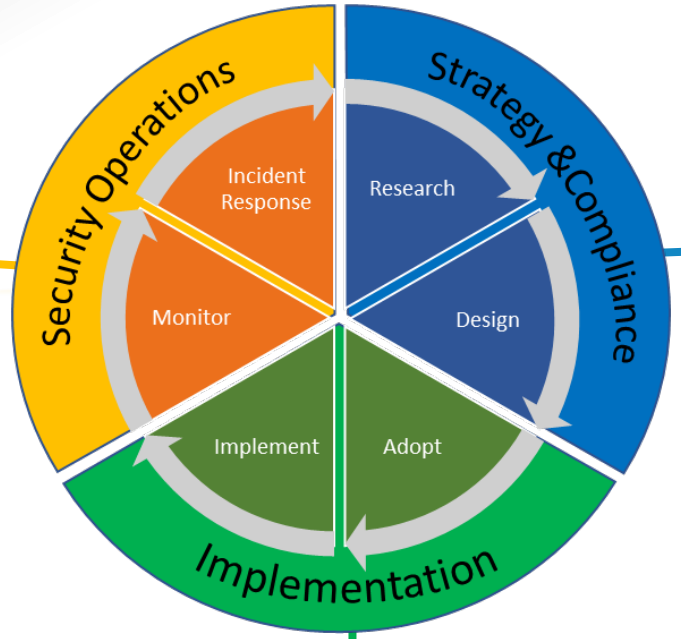
Monitor

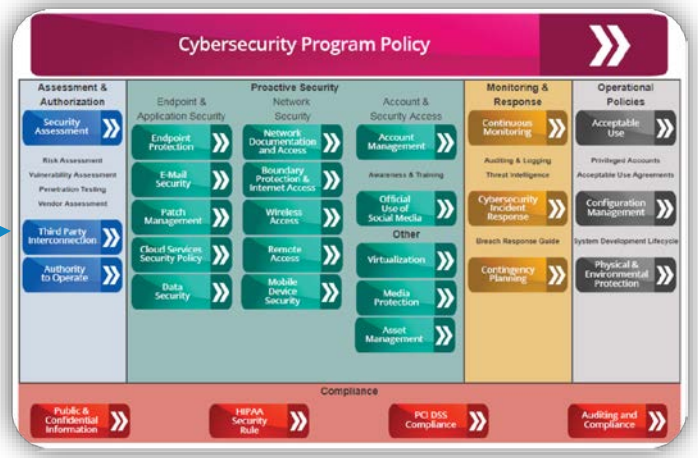
SKYLINE TECHNOLOGY SOLUTIONS

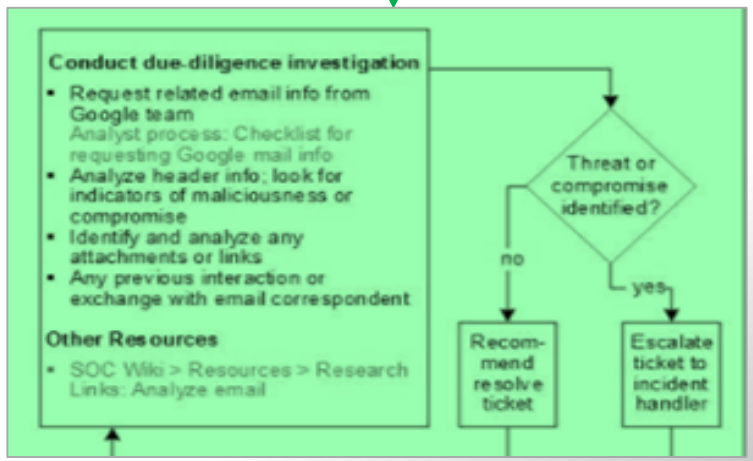
Incident Response



What does a mature program look like?







SKYLINE TECHNOLOGY SOLUTIONS

Organizations with an Established Program

- Audit to check whether personnel, technology, and processes are in line with Program Requirements
  - Automatic
  - Manual
- Create a compliance division and routinely check status and identify improvements

Where Does My Organization Start?

- Where does my organization stand today?
- How do I find out if my organization has a program?
- Who should I contact?

Review

- Why – Risk,
- What – Definition and Resources that offer Frameworks
- How – Programs take energy, resources, and 24/7 attention

Questions?