Welcome to Colorado Springs

Compliance vs. Cybersecurity

- How many remember the massive computers in the huge computer rooms?
  - What were the advantages?
  - What were the disadvantages?

Chat about one solution

- National Institute of Standards and Technology (NIST)
  - U.S. Department of Commerce

What has NIST provided?

- Cybersecurity Framework
  - https://www.nist.gov/cyberframework

Framework Functions

- Identify
- Protect
- Detect
- Respond
- Recover

Categories within Functions

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 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)

Do Not Panic!!!

- Isn’t that just like IT folks, wanting to use acronyms everywhere!?!?!?!

Categories within Functions

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 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)

ID.AM

- The data, personnel, devices, systems, and facilities that enable an organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Categories within Functions

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 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)

RS.AN

- Analysis is conducted to ensure adequate response and support recovery activities.

Categories within Functions

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 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)

DE.DP

- Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Categories within Functions

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 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)

RC.IM

- Recovery planning and processes are improved by incorporating lessons learned into future activities.

Where does one go from here?

Questions

DRickard@SpringsGov.com