Compliance vs. Cybersecurity

MARK LINTON

PRESIDENT, FINGARDE

Transparency

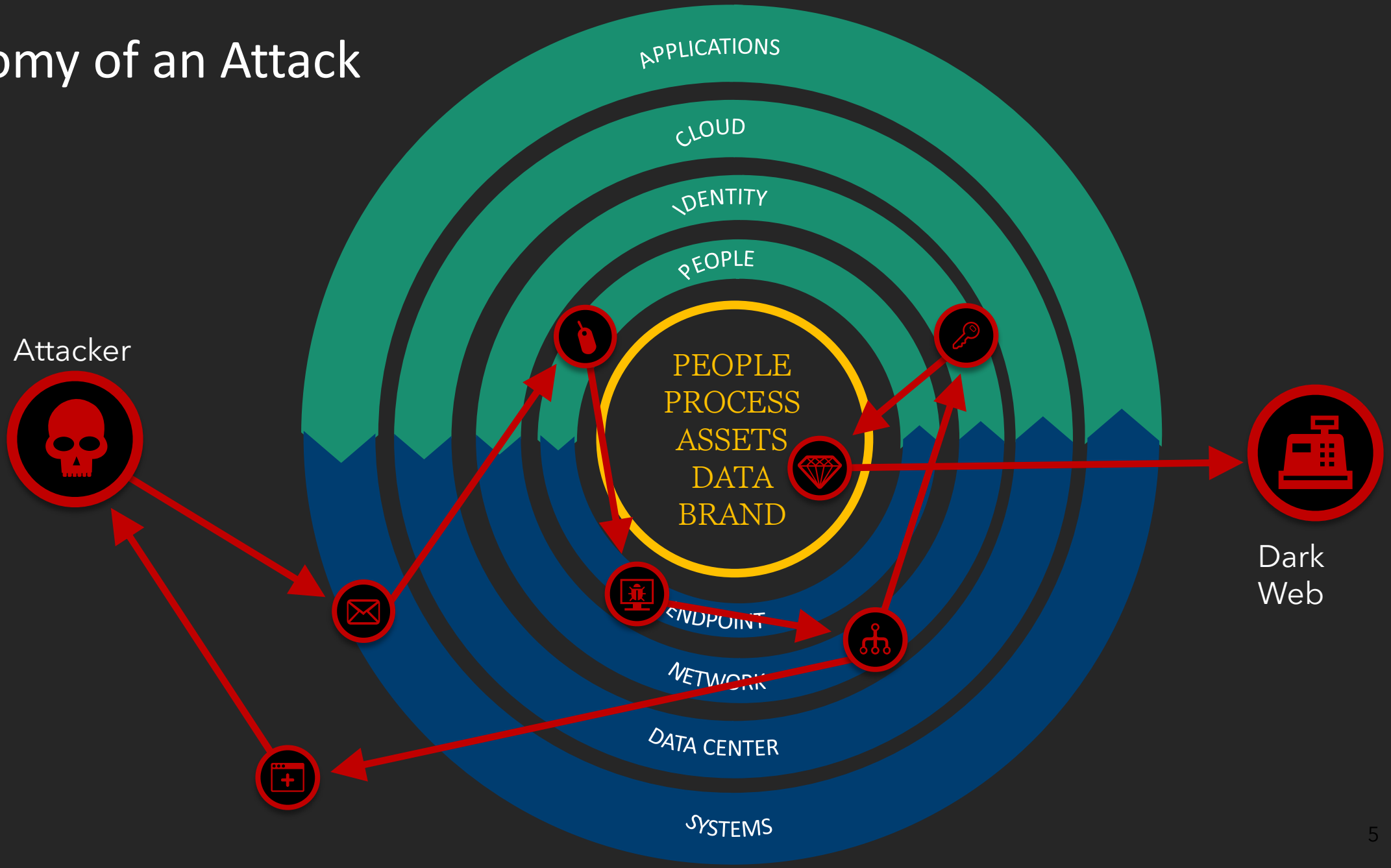
1. FinGarde is a Platinum Sponsor of the FPA of Central Ohio
2. We have active clients on this call.
3. I am not your insurance agent, legal team, or compliance officer.
4. I assume that you are working with a technology company to manage your environment.
5. We are looking at this topic through the lens of information technology.
6. Tools/Brands mentioned are for reference only, focus on the solution more than the brand.

Overview

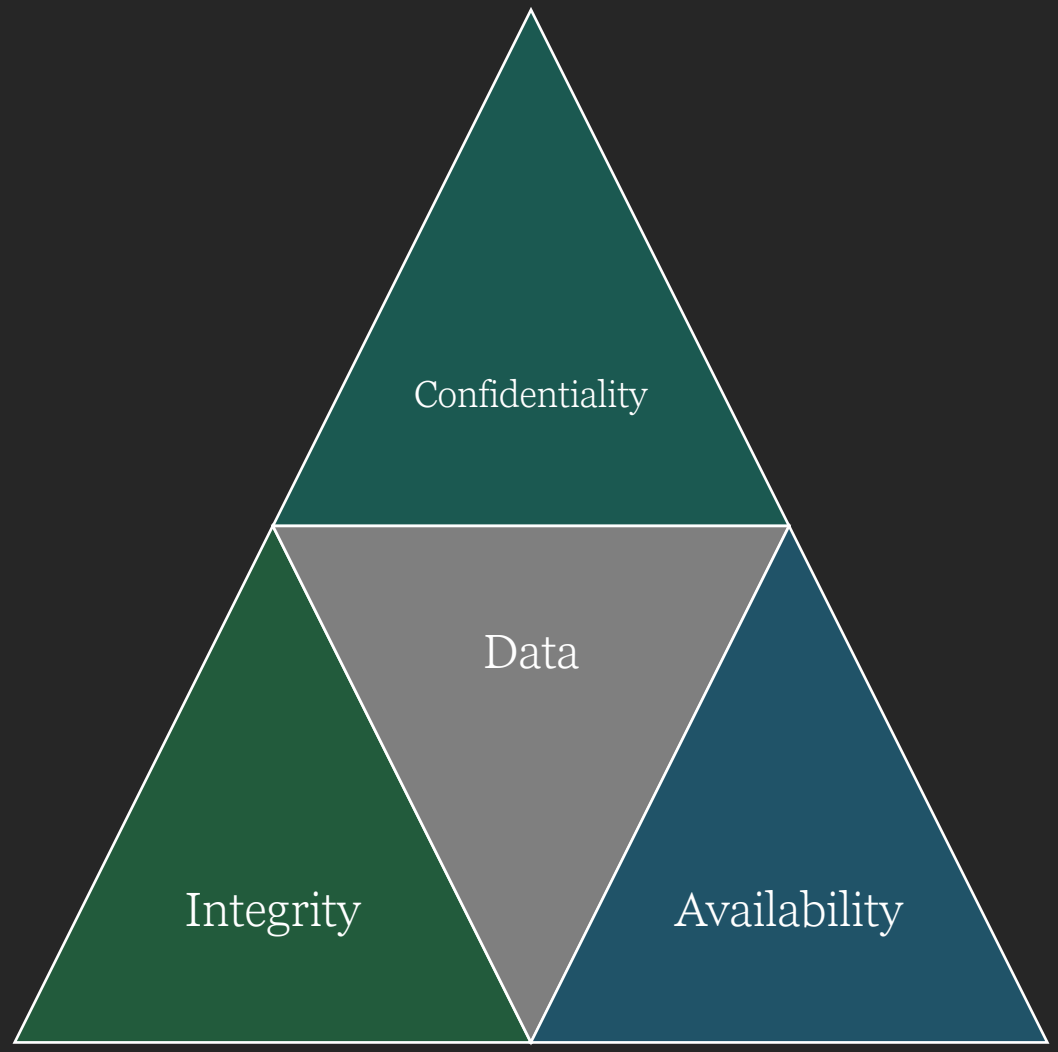
- High level overview of Cybersecurity (for context).
- Risk Assessments
- Frameworks
- Controls
- Questions/Discussion

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Anatomy of an Attack



CIA Triad



CIA in Practice

- **Confidentiality:** When using an ATM, you will need your ATM/Bank card (something you have) and your PIN (something you know) before you can execute a transaction.

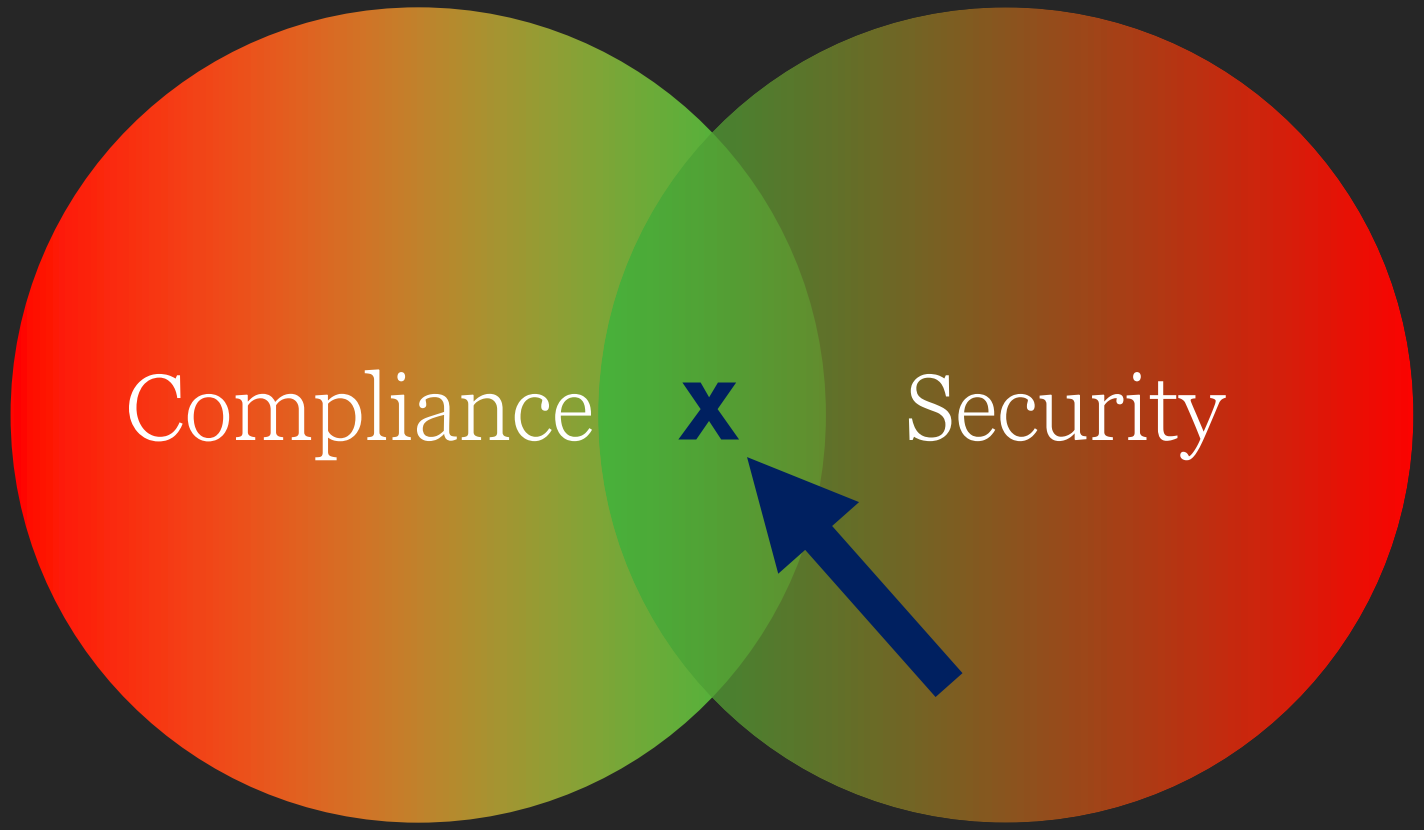
- **Integrity**: Bank software and accounting systems will ensure data integrity (your transaction information is successfully recorded to your bank account).

- **Availability**: The ATM provides the availability of banking resources day or night.

Compliance involves meeting various controls (usually enacted by a regulatory authority, law, or industry group) to protect the confidentiality, integrity, and availability of data.

Do Compliance and Security Controls natively move away from, towards or with one another?

Goal: Find X

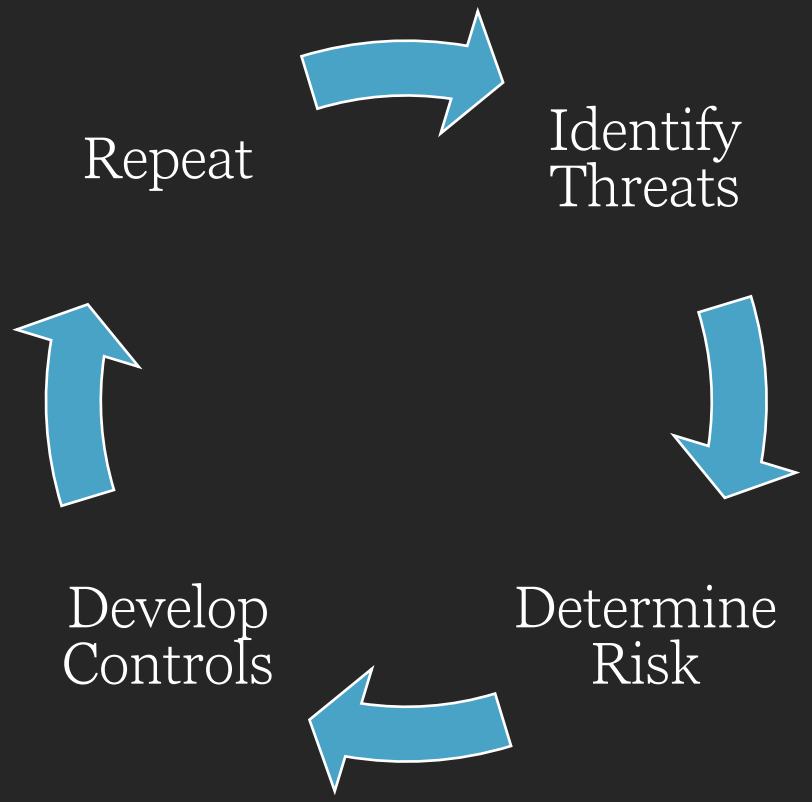


Step #1: Complete a Cybersecurity Risk Assessment

The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.

- NIST Definition

In English...



Identify:

Do you store, use or transmit personally identifiable information (PII) (e.g., social security numbers or date of birth) or firm sensitive information (e.g., financial records) electronically?

Thought Exercise

Determine Risk:

Sensitive Data	Location	Risk Level
Performance Reports	DropBox	Medium
Client SS#	Cloud Hosted CRM	High

Thought Exercise

Develop Controls:

- User Access Policy (Administrative Control)
- Restrict Access Based on Role (Technical Control)


Burden
Policies, Procedures and Controls
Risk

Step #2: Choose a Framework

A cybersecurity framework is a collection of best practices that an organization should follow to manage its cybersecurity risk. A strong cyber risk management framework is closely intertwined with the organization's risk management strategy and risk management programs.

Common Cybersecurity Frameworks

- Center for Internet Security (CIS) – CIS Controls
- National Institute of Standards and Technology (NIST) – CSF / SP 800-53
- International Organization for Standardization (ISO) – 27001, Information Security Management.
- *The Securities and Exchange Commission (SEC)*
- *Financial Industry Regulatory Authority (FINRA) – 3110, 3210, 4530(b), 4530.04*

Cybersecurity and the SEC

In the United States, aspects of cybersecurity are the responsibilities of multiple government agencies, including the SEC. Just in the financial services space, there are a myriad of regulators that oversee registrants with differing requirements and obligations.[1] Because of this, it is not uncommon for market participants under the SEC's jurisdiction to be subject to multiple authorities' obligations regarding cybersecurity, including obligations to report to a federal agency or to the public.

But the SEC has an important interest in cybersecurity, which has a nexus to every part of the SEC's three-part mission: to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. For example, securing investors' account data is a clear prerequisite for investor protection. The market integrity that characterizes fair, orderly, and efficient markets requires, at the very least, reliable clearing and settlement, which relies on secure data. And, of course, security is the foundation on which a stable and growing economy is based.

https://www.sec.gov/news/speech/roisman-cybersecurity-102921

Comparison

- **SEC:** Provide a copy of Adviser's cybersecurity training policies and procedures.

- **NIST CSF:** ID.GV-1: Organizational cybersecurity policy is established and communicated

  - CIS CSC 19
  - COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02
  - ISA 62443-2-1:2009 4.3.2.6
  - ISO/IEC 27001:2013 A.5.1.1
  - NIST SP 800-53 Rev. 4 -1 controls from all security control families

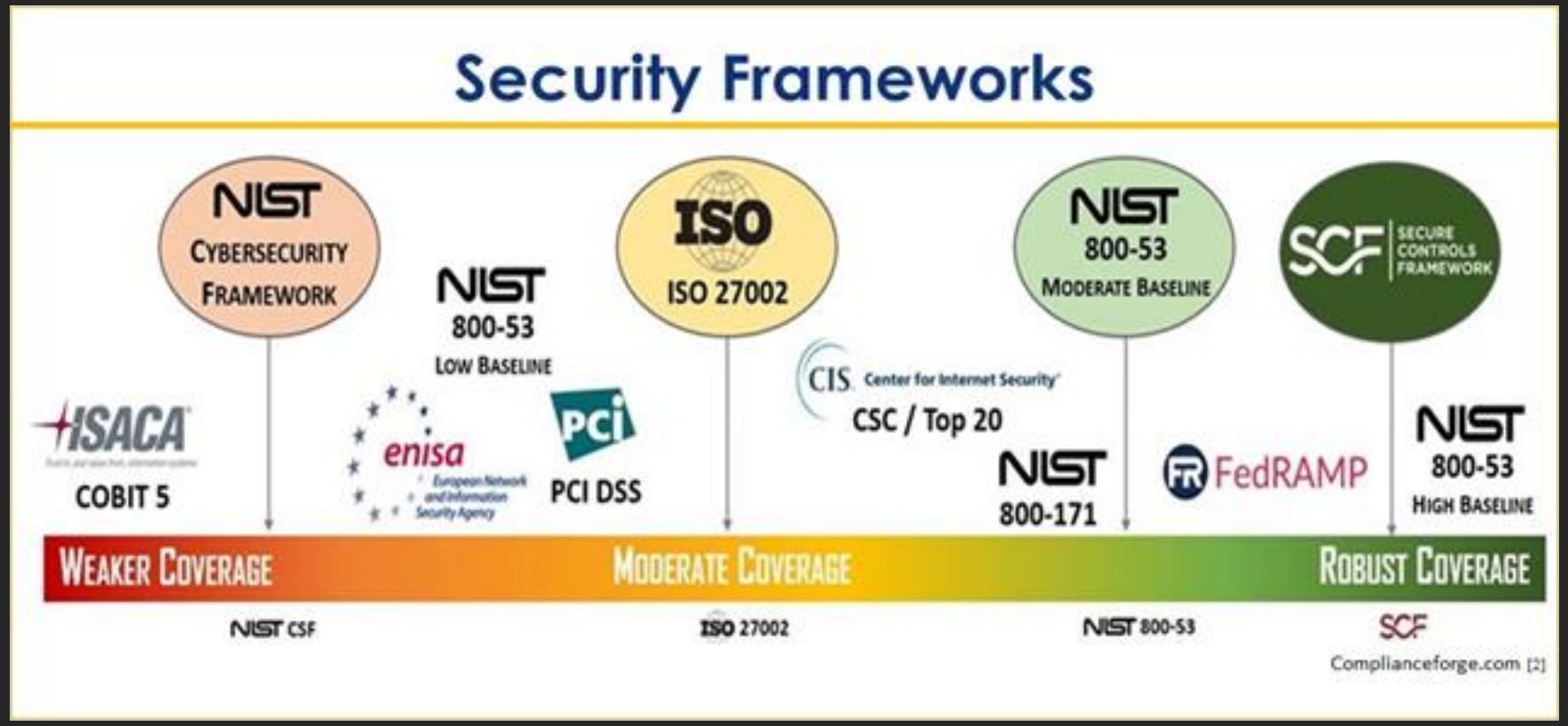
Audit Question (example):

- Provide a copy of Adviser's policies, procedures, and standards regarding any devices (i.e., Adviser issued and personal devices) used by employees, IARs, contractors/vendors, and/or other third parties to access Adviser's system externally including any written policies or procedures addressing the encryption of such devices and the Adviser's ability to remotely monitor, track, and deactivate remote devices.

Policy needed: Mobile Device Management (Corporate and Personally Owned)
- Framework: various

Tools Needed:
- Mobile Device Management Software

Framework Coverage



Step #3: Deploy Administrative and Technical Controls

Administrative (Policies and Procedures)

- Disaster Recovery Plan
- Business Continuity Plan
- Compliance Manual
- Acceptable Use Policy
- Mobile Device Policy
- Password Policy

Technical (Configurations and Tools)

- Cloud Infrastructure / Backup
- Configuration Management / Filtering
- Mobile Device Management
- Application Whitelisting
- Multi-Factor Authentication
- Password Management Software

Audit Question

Provide a copy of Adviser's written plan that addresses prevention, detection, and mitigation of the effects of a cybersecurity incident and/or recovery from such an incident, including any policies for addressing responsibility for losses associated with attacks or intrusions impacting clients, if such a plan exists. If Adviser maintains separate written cybersecurity incident response policies and procedures, please provide a copy.

PR.AC-1 (NIST CSF)

Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.

Supporting Frameworks

- CIS CSC 1, 5, 15, 16
- COBIT 5 DSS05.04, DSS06.03
- ISA 62443-2-1:2009 4.3.3.5.1
- 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
- ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3
- NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11

Policies and Procedures

- Least Privilege – each team member is given the least amount of access possible to do their work.
- Separation of Duties – checks and balances
- Account Life Cycle – Accounts are Created at onboarding (HR Process), deprovisioned at termination (HR Again) and monitored while in use (IT Department)

Technical Controls

- Security Information and Event Management (SIEM) with properly configured rules and alerts.
- Geolocation/IP restrictions
- Multi-Factor Authentication

Policy Templates

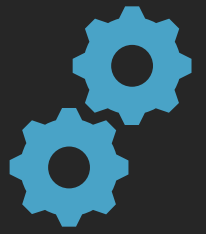
- SANS: https://www.sans.org/information-security-policy/
- CIS Guide: https://www.cisecurity.org/wp-content/uploads/2020/07/NIST-CSF-Policy-Template-Guide-2020-0720-1.pdf

Quick Reference

- FINRA Cybersecurity Checklist: https://www.finra.org/compliance-tools/cybersecurity-checklist
- NIST CSF: https://www.nist.gov/cyberframework/framework
- NIST SP 800-53: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
- SEC Cybersecurity: https://www.sec.gov/spotlight/cybersecurity

Complete a Risk Assessment

Choose a Framework



Deploy Administrative and Technical Controls

Recap

Questions?