rkl ADVISORS for WHAT'S NEXT

Staying Ahead of Ever-Changing Security Compliance Standards

Presented by: Michael McAllister | Partner, IS Assurance & Advisory Group

What Will We Introduce

01.

Regulatory Expectations

When working with your regulatory parties, it is important to understand their current stance and what they might be expecting.

02.

IT Security Standards / Frameworks

Having the right IT security framework established within your business is critical, but which one would fit you best and why are they important?

03.

Common Controls

What are some of the common control struggles that companies have regarding implementation and documentation?

Welcome and Meet Your Team

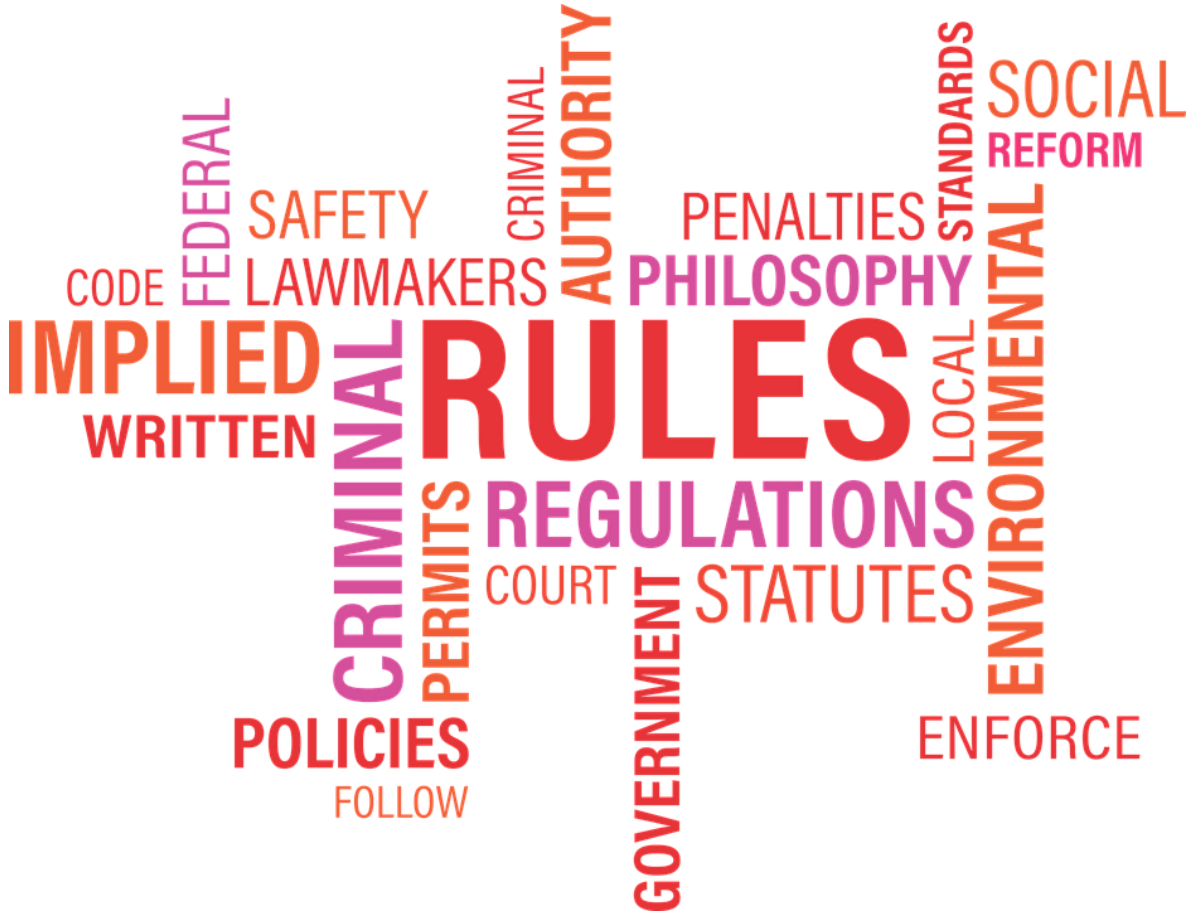
Michael McAllister, CPA. CITP, CISA

Partner, IS Assurance and Advisory Services

Michael McAllister serves as the Partner for RKL's IS Assurance and Advisory Services Group, with his focus on supporting the accounting world and helping clients navigate through the issues and concerns that may keep them up at night. With more than 25 years of experience in accounting and information security, Michael builds the knowledge bridge between the financial aspects of accounting, and the information technology systems and controls that support each process. Together with his IS Assurance and Advisory Services team, he serves clients in a variety of industries, ranging from manufacturing to retail, technology and financial institutions; providing information technology internal audits, IT governance reviews, cybersecurity assessments, and compliance evaluations with various IT security standards.

Regulatory Expectations

- Recent regulatory trends regarding Information Technology
- New SEC proposal for cybersecurity



Recent regulatory trends regarding Information Technology

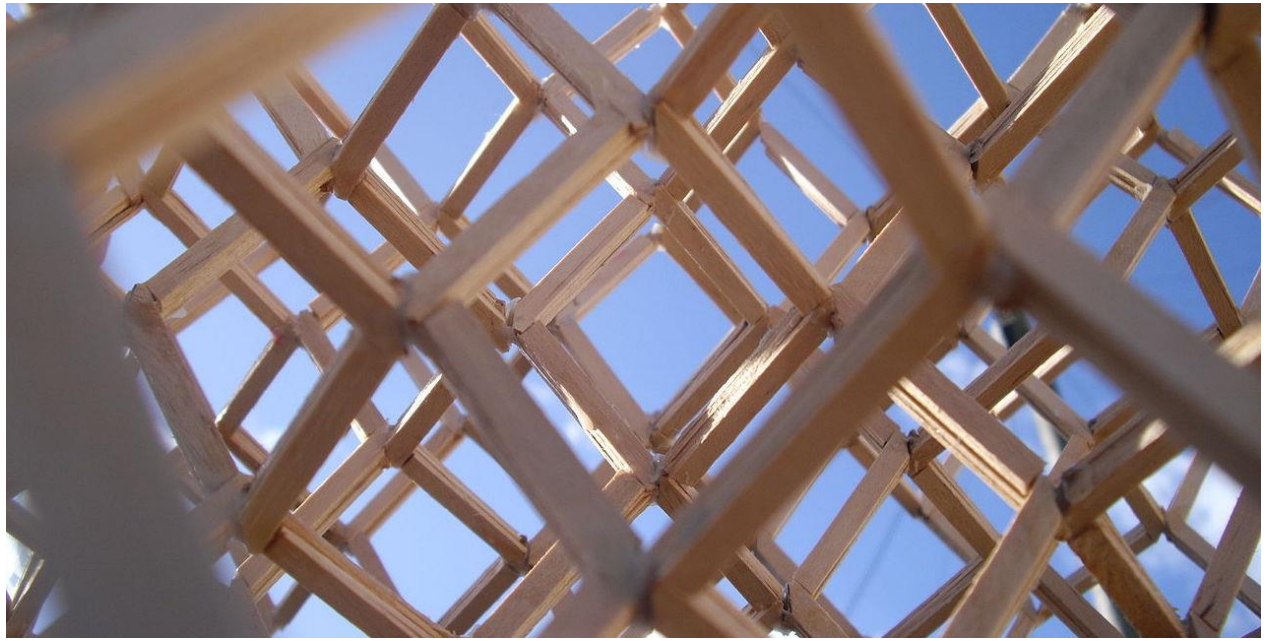
- Regulators recognize the need to connect the digital work with the financial industry
- Regulatory reform by 2025, an uphill battle
- Effective April 1, 2022 – 36 hour notification on computer-security incident

New SEC proposal for cybersecurity

Public comment phase of a new cybersecurity proposal from the SEC.

- Reporting current status on previous material cybersecurity incidence
- Registrants requirement to identify and manage cybersecurity risks
- Board of Director's oversight of cybersecurity risk

IT Security Standards / Frameworks



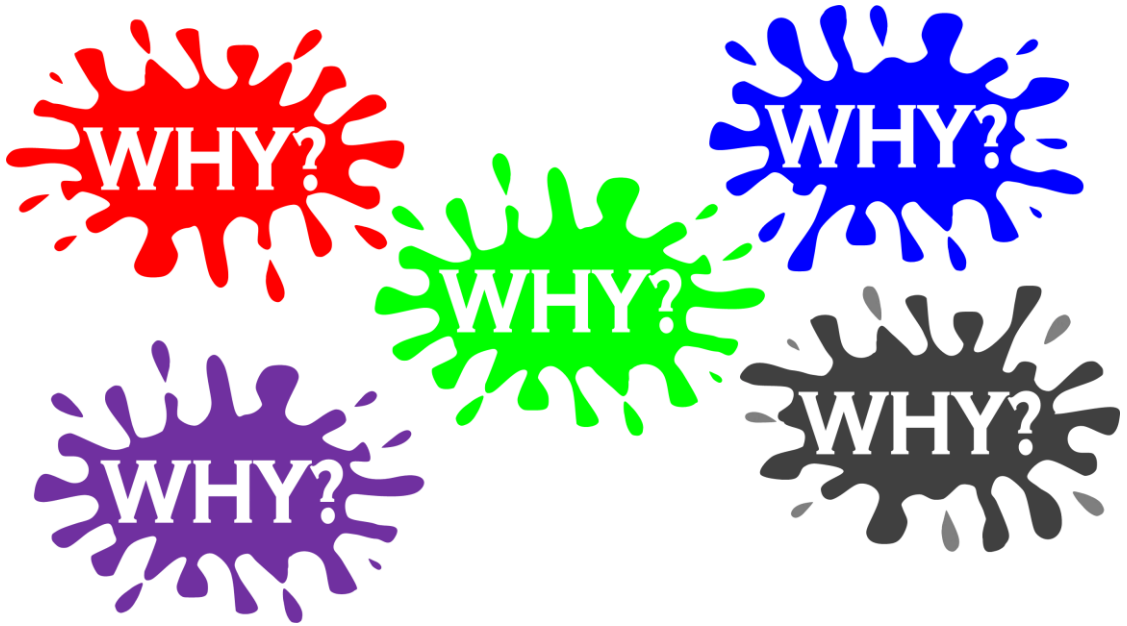
Standards / Frameworks

Why are Frameworks Important?

What is the difference between Frameworks and Standards?

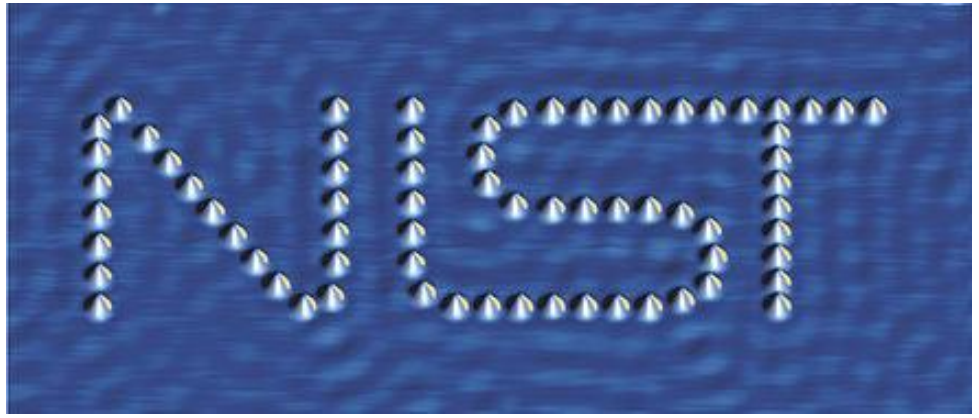
- National Institute of Standards and Technology (NIST)
- International Organization of Standards (ISO)
- Payment Card Industry Data Security Standard (PCI DSS)
- System and Organizational Control (SOC) reports

Frameworks – Why are they important?



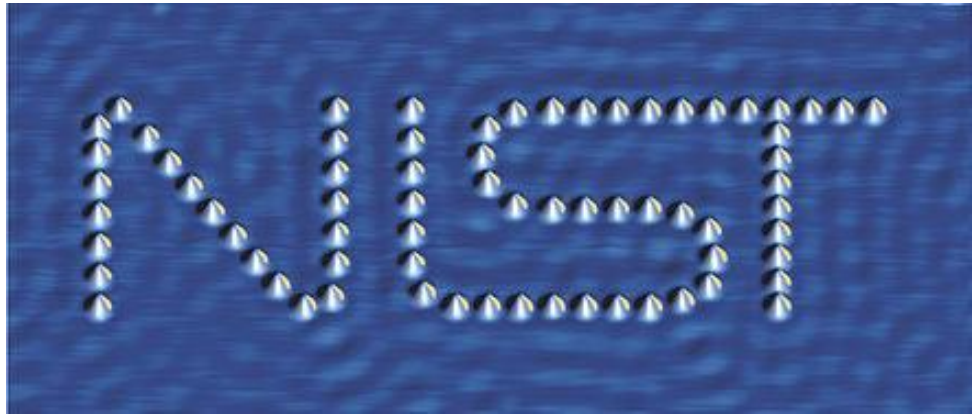
- Great starting point for establishing good policies, procedures and operational activities
- Reduces the risk and impact of cybersecurity issues
- How do you chose the right one?

National Institute of Standards and Technology (NIST)



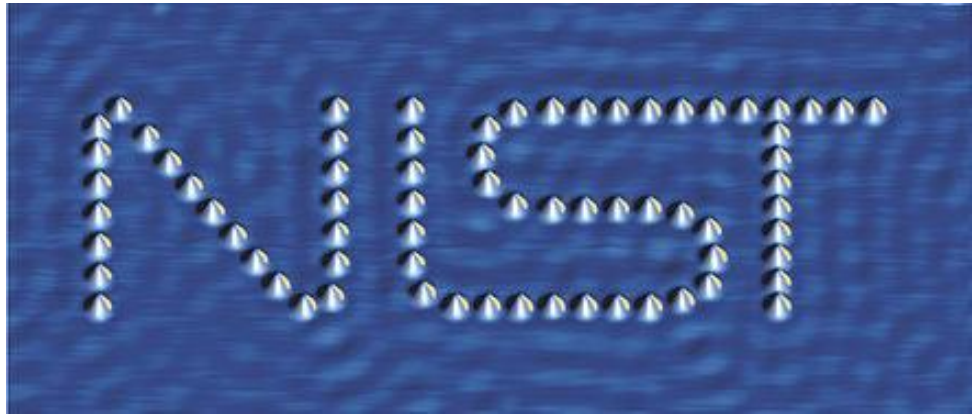
- NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

National Institute of Standards and Technology (NIST) – SP 800-53



- Customizable to fit the organization
- Updated December 2020
- Comes in three flavors:
  - Low baseline (149 controls)
  - Moderate baseline (286 controls)
  - High baseline (369 controls)
  - Total number of controls - 1007

National Institute of Standards and Technology (NIST) – SP 800-53

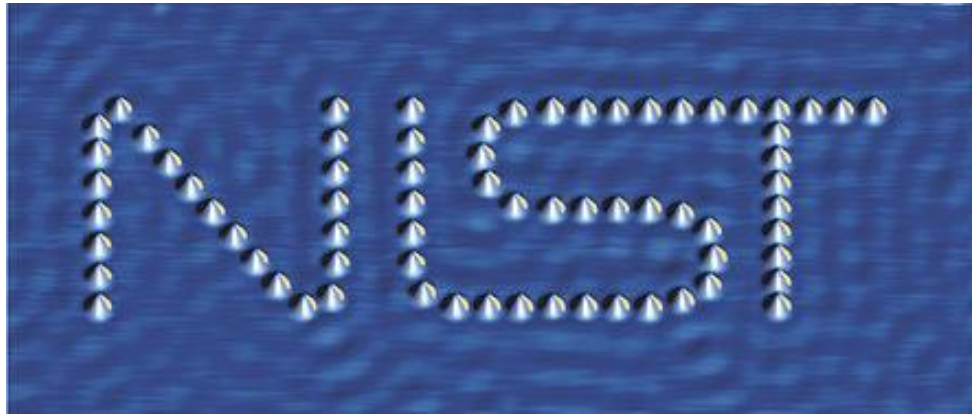


- Control Families

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

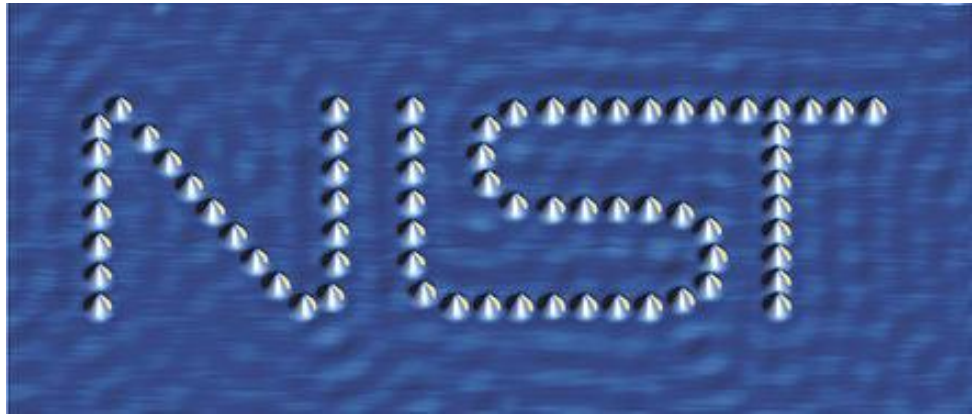
ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

National Institute of Standards and Technology (NIST) – SP 800-171



- Derived from FISP 200 and moderate baseline of SP 800-53
- Established in 2016
- Updated February 2020
- Purpose – Provide federal agencies with recommended security requirements to protect confidentiality of Controlled Unclassified Information (CUI)

National Institute of Standards and Technology (NIST) – SP 800-171

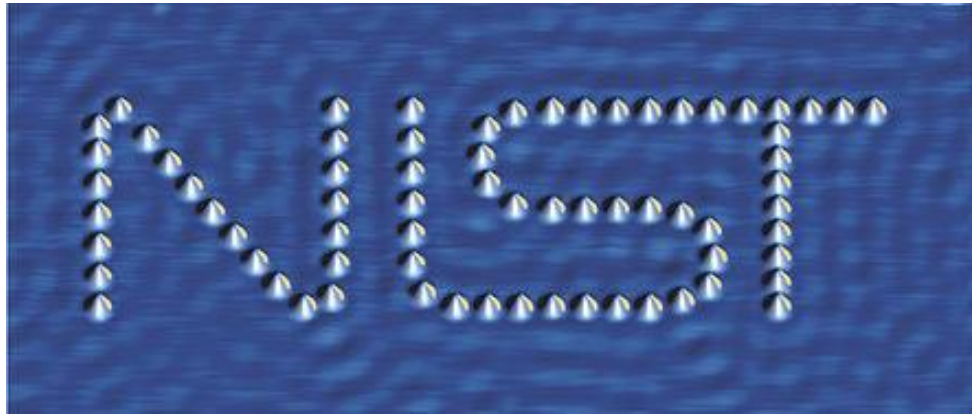


Control Families

TABLE 1: SECURITY REQUIREMENT FAMILIES

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

National Institute of Standards and Technology (NIST) – SP 800-171



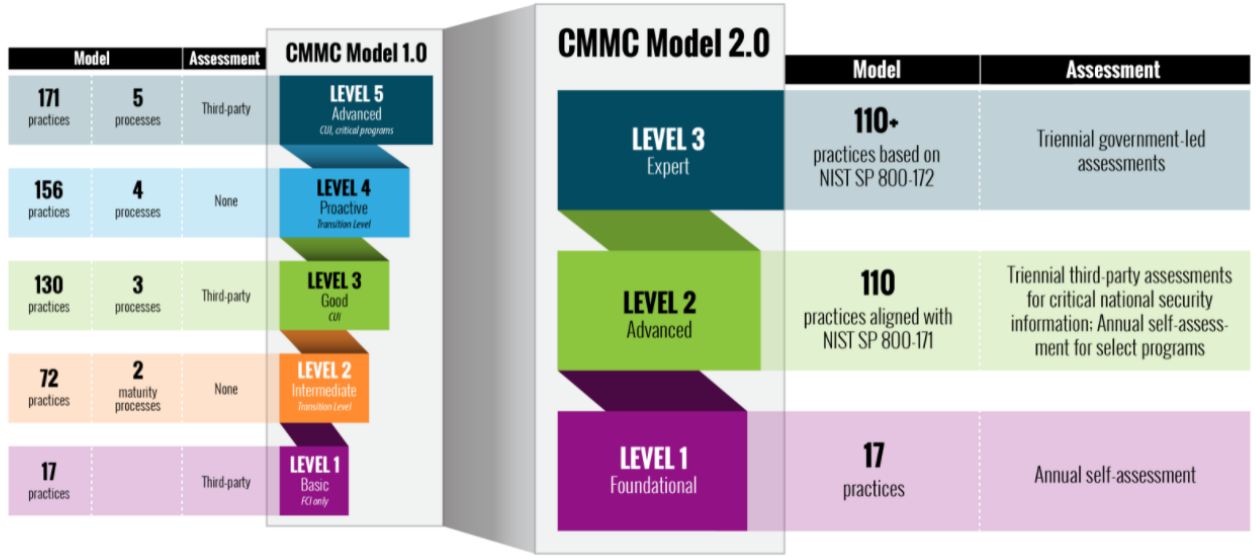
- Number of controls – 110
- The recommended security requirements contained in this standard are only applicable to a nonfederal system or organization when mandated by a federal agency in a contract, grant, or other agreement.
- Used as the base for CMMC

Cybersecurity Maturity Model Certification

- January 30, 2020 - CMMC Released
- November 4, 2021 – CMMC 2.0 Announced
- 9-24 month rulemaking process completion
- Contracts are expected to be released as soon as rulemaking process is complete (Approx. 7/22 – 11/23)

Cybersecurity Maturity Model Certification

KEY FEATURES OF CMMC 2.0



International Organization of Standards (ISO)

- ISO 27000 information security framework for all types and sizes of organizations
- Published 2005
- Over 60 standards covering a broad spectrum of Information security issues

International Organization of Standards (ISO)

- ISO 27001
  - Introduced 2013
  - Formally specifies an Information Security Management System (ISMS)
- Risk-driven approach

International Organization of Standards (ISO)

- ISO 27002 specifies the code of practice for developing information security controls
- Comprehensive assessment is necessary to determine applicable controls
- Number of controls - 93

International Organization of Standards (ISO)

Control domains (4)

- Organizational (37 controls)
- People (8 controls)
- Physical (14 controls)
- Technical (34 controls)

Payment Card Industry Data Security Standard

- Released December 2004
- Purpose – ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment
- Version 4.0 issued on March 31, 2022
- What has changed with the new version?

Payment Card Industry Data Security Standard

PCI DSS COMPLIANT

Table 1. Principal PCI DSS Requirements

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	**1.** Install and Maintain Network Security Controls. **2.** Apply Secure Configurations to All System Components.
Protect Account Data	**3.** Protect Stored Account Data. **4.** Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	**5.** Protect All Systems and Networks from Malicious Software. **6.** Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	**7.** Restrict Access to System Components and Cardholder Data by Business Need to Know. **8.** Identify Users and Authenticate Access to System Components. **9.** Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	**10.** Log and Monitor All Access to System Components and Cardholder Data. **11.** Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	**12.** Support Information Security with Organizational Policies and Programs.

System and Organizational Control (SOC)

SOC 1

- Used for services that are material to financial reporting
- Control Objectives

SOC 2

- Trust Categories
  - Security, Availability, Confidentiality, Processing Integrity, and Privacy
- Criteria

System and Organizational Control (SOC)

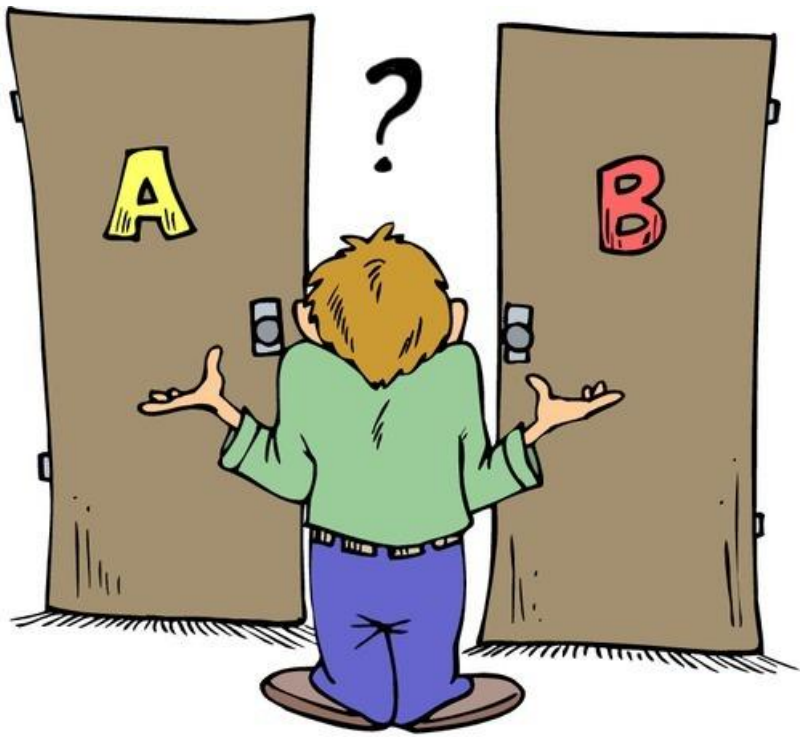
SOC for Cybersecurity

- Cybersecurity risk management reporting framework
- General use
- Differences from SOC 2?

SOC for Supply Chain

- Trust Categories
  - Security, Availability, Confidentiality, Processing Integrity, and Privacy

Frameworks



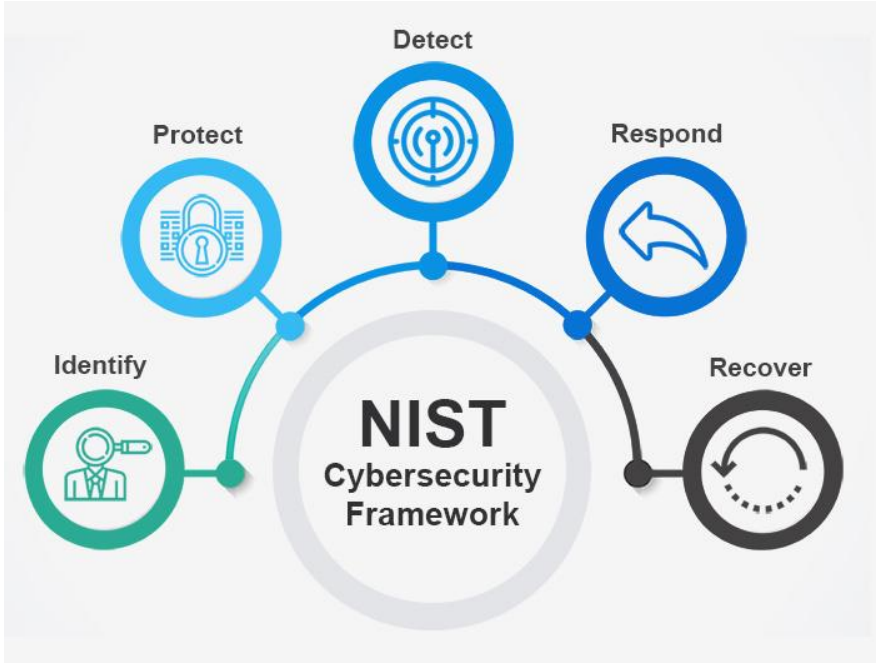
Other Framework options:

- COBIT
- NIST CSF

Control Objectives for Information Technology (COBIT) Framework

- Is the most used framework to achieve Sarbanes-Oxley compliance
- Distinguishes between risk governance and risk management activities
- Components:
  - Evaluate, Direct and Monitor
  - Align, Plan and Organize
  - Build, Acquire and Implement
  - Deliver, Service and Support
  - Monitor, Evaluate and Assess

National Institute of Standards and Technology (NIST) – Cybersecurity Framework



- NIST CSF – focuses on risk analysis and risk management
- Broken down into 24 Categories
- 109 subcategories
- Cross-references to other standards

Having the right standard / framework does not solve all risks

Additional considerations when selecting and implementing any IT security standard / framework:

- What is being asked of the company from the end users and why?
- Cost benefit / Return on Investment
- Establishing procedures / controls that are repeatable
- Setting the right expectations

Common Controls

- Awareness Training
- Configuration Management
- Incident Response
- Risk Assessment
- Outsourcing / Vendor Management

Awareness Training

- Social Engineering
- Employee security training

Configuration Management

- Source coding / change management
- Patching
- System parameters / Confirmation management

Incident Response

- Business Continuity Plan does not equal an Incident response Plan
- The need for testing

Risk Assessments

- Informal practices
- Consideration of risk and rewards
- External threats
- Annual review and bringing the right group to the table

Outsourcing / Vendor Management

- Types of risk associated with outsourcing services
- Transfer of risk
- Holding outsourced provider accountable

Outsourcing - Types of Risks

- Risks related to the function outsourced
  - Sensitivity of data accessed, protected, or controlled
  - Volume of transactions
  - Criticality to the company's business
- Operational or transaction risks
  - Fraud
  - Errors
  - Inability to deliver products or services
- Reputational risks
- Strategic risks
- Compliance risks

Outsourcing - Transfer of Risk

- Senior management and Board awareness of the risk associated with outsourced agreements
- Ensure that the outsourcing is worth the risk involved.
- Implement effective controls to address and identify risks
- Perform ongoing monitoring to identify and evaluate changes in risks
- Document procedures, roles/responsibilities, and reporting mechanisms
- **Ultimately – the risk of the inability to provide services still resides with you.**

Outsourcing - Holding Outsourced Service Providers Accountable

Critical Vendor

- SOC reports
- Financial reports
- Performance evaluations
- Internal controls environment

SOC Report Available?

Two types of SOC reports:

- SOC 1
- SOC 2

Different version:

- Type 1
- Type 2

Outsourcing - Holding Outsourcing Service Providers Accountable

Down the Rabbit Hole

- Does the subservice cover key control objectives?
- Were the Complementary Service Organization Controls (CSOCs) reviewed?
- Can you get access to the reports?

Alternative Procedures

- How does the vendor control logical access?
- How are change management controls implemented?
- What kind of network security controls have been implemented?
- What are the controls around any specific business process they provide?
- Contact the vendor for an onsite or remote visit to review the controls and supporting documentation

Do You Have Questions?

rkl ADVISORS for WHAT'S NEXT

Thank You for Joining Us

Whatever your next move, we're here to help.

Michael McAllister
mmcallister@rklcpa.com