Understanding

SOC2 Reports

Types, Purposes, & Key Benefits Explained

MUELLER

RSI

MUELLER

Certified Public Accountants
Business & Financial Advisors

Chicago Metropolitan Area (Headquarters) & Sarasota, Florida

Founded in 1968

- Business, accounting, tax, assurance, and financial advisory firm
- Domestic and international clients in a variety of industries, including:
  - Publicly traded companies
  - Local governments
  - Not-for-profit organizations

Nation's Premier Cybersecurity and Compliance Provider

San Diego, California

Founded in 2008

- Cybersecurity
  - Managed Security Services
  - Cyber defense
    - Penetration Testing
- Compliance
  - Healthcare (HITRUST, HIPAA)
  - Payment (PCI, FINRA)
  - Federal (CMMC, NIST800-171)
  - Data Privacy (GDPR, CCPA)

Drent Shields
CPA, MBA, CISA, CITP
Partner
Mueller

Kyle Wehrli
CPA, CISA, CITP
Audit Manager
Mueller

Nick Padron
Senior Security Consultant
RSI Security

What is a SOC Report?

- System and Organization Controls (SOC) report
- Audit of internal controls relevant to a service organization's defined system
- Only a Certified Public Accountant can issue
- Contents:
  - Auditor's Opinion
  - Service Organization's Assertion
  - Service Organization's System Description
  - Auditor's Test of Controls (Type 2 Only)
  - Other Information Provided by Service Organizations (Optional)

SOC Terminology

- Service Organizations
- Subservice Organizations
- User Entity
- SAS 70 (Superseded)
- SSAE16 (Superseded)
- SSAE18 (Current)

SOC Reports Summary

	SOC 1	SOC 2 / 3	SOC for Cybersecurity	SOC for Supply Chain
Criteria	ICFR[1]	AICPA Trust Services Criteria	Cybersecurity Risk Management Program[2]	AICPA Trust Services Criteria
Scope	Specified System	Specified System	Entity-Wide	Production, Manufacturing or Distributions Systems
Primary Audience	Existing Customers and their Auditors	Existing & Prospective Customers, Business Partners[3]	General Use	Existing & Prospective Customers, Business Partners

[1] Internal Controls over Financial Reporting
[2] AICPA Trust Services Criteria or other suitable criteria (e.g. NIST CSF or ISO 27001)
[3] SOC 3 is a appropriate for general use.

Which SOC Audit is Right For You?

SOC 1

- Payroll Processing
- Claim Processing
- Collections Processing
- Medical Billing
- Employee Benefit Plan Administrators
- AR/AP Processing
- Professional-Law & Accounting

SOC 2

- Data Centers
- Application Hosting Firms
- Co-location Center Firms
- Managed Security Service Providers (MSSP)
- Cloud-Based Software-as-a-Service (SaaS)

Type 1 vs Type 2 Reports

Content	Type 1	Type 2
Period of Coverage	Point-In-Time	Period-Of-Time
Opinion Provided On:		
Suitability of Design	X	X
Implementation of Controls	X	X
Operating Effectiveness		X

The Trust Services Categories

- Security (Common Criteria)
- Availability
- Processing Integrity
- Confidentiality
- Privacy
- Additional SOC 2 Add-Ons

Becoming SOC Compliant

Readiness Assessment

- Interviews and walkthroughs
- Documentation of controls currently in place
- Identify gaps and weaknesses
- Draft of service organization's system description

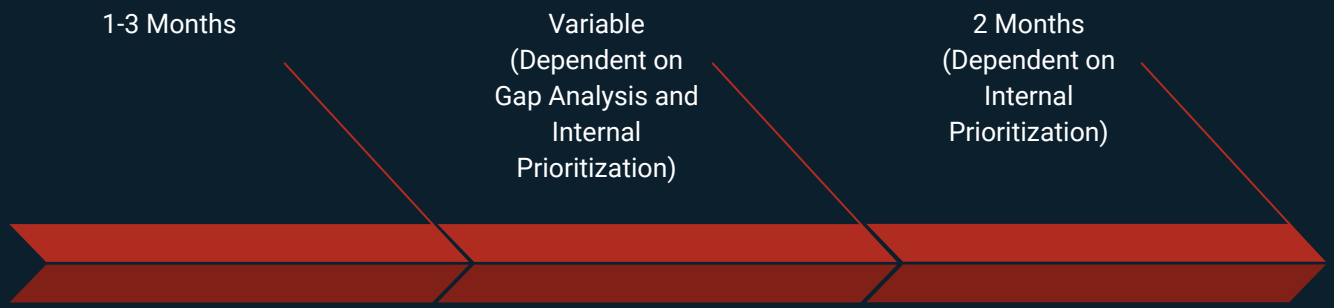
Remediation

- Addressing gaps and weaknesses
- Preparing for audit

Undergoing Audit

- Selection of audit firm
- Decision of a Type 1 versus a Type 2 audit
- Commencement of audit

Typical Timeline



Readiness Assessment

Performed by security consultant and the service organization

Remediation

Performed by the service organization with the assistance of a security consultant

Type 1 Examination

Performed by a CPA firm and the service organization

Initial SOC Compliance Challenges

01	**Incomplete or ineffective risk assessment**	Controls should be designed to address the unique risks in your environment
02	**Lack of documented policies and procedures**	Leads to inconsistent execution and application of controls by personnel
03	**Resource constraints for initial SOC readiness and remediation work**	Leads to low level of priority and creates lag in completion
04	**Lack of executive buy-in**	Leads to low level of priority and creates lag in completion
05	**Inadequate documentation of performance of controls**	May lead to inefficient audit testing and potential audit findings
06	**Inconsistent execution of controls while under audit**	Will result in audit findings and potential qualifications
07	**Lack of transparency**	Will result in inefficient and incomplete readiness assessment and potential audit findings/qualifications

What is Risk?

Security is never "perfect"

Year over Year, continually assess risk

Higher Risk
Lower Cost
Lower Maturity

Goal is to build a sustainable security and technology program that balances the need to protect and run the business

Lower Risk
Higher Cost
Higher Maturity

Common Risks & Security Services

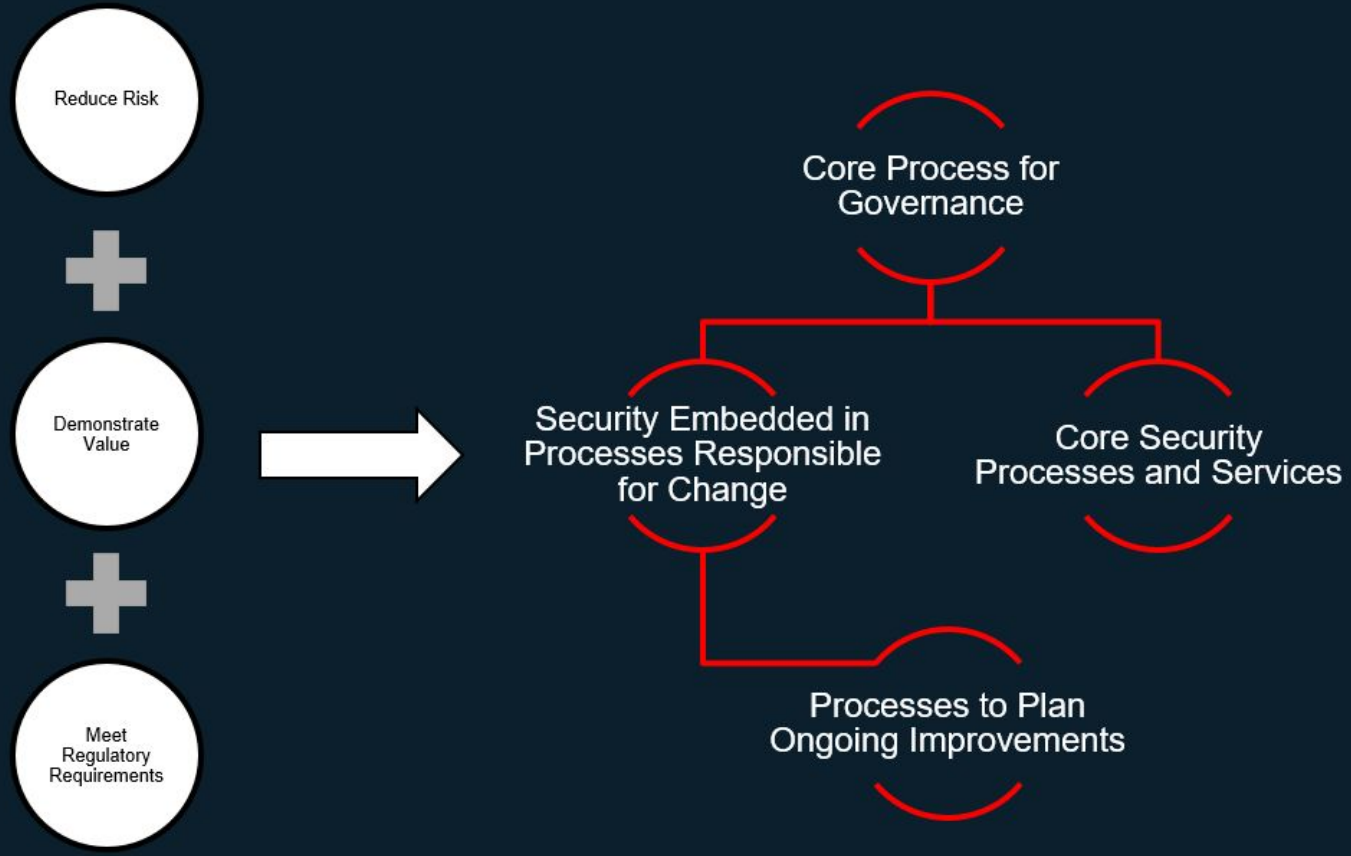
Cybersecurity & Technology Risks	Security Services & Processes
Loss of the following Data Records: • Corporate • Customer • Employee	• Quarterly review of user access • Workflow authorization for access to data • Security systems and 24/7 monitoring
Regulatory Compliance: • SOX • GDPR • CCPA	• Annual external/internal audit • Business partnerships with Accounting, Sales, Marketing, various business units, and IT to ensure annual compliance
Emerging Technology & New Risks: • Mobile technology increases ways to access systems and data • Internet of Things (IoT) introduces adhoc abilities to collect data • Cloud technology easily procured by anyone	• Business to IT Strategic Alignment • Ensure IT is involved with all technology procurement and decisions • Engage industry thought leaders to aid in future technology and information management

Cybersecurity Risk Management

5 Focus Areas

- Formalize **Risk Assessment** process by analyzing threats and their potential business impact
- **Assess** impact of existing **Controls** to address threats and help enhance existing controls or implement new ones
- **Risks** are dynamic and should be **Tracked** in a risk register to provide visibility to stakeholders, board of directors, internal/external audits, and regulators
- Establish roles and responsibilities for **Risk Decision Making** to enhance strategic and tactical risk management capabilities
- Create a risk-aware culture through **Accountability** by making good risk-based decisions through establishing risk management processes

Assess, Prioritize, & Implement Security



Critical Security Services & Processes

Document & Deliver Critical Security Services & Processes

- Security governance ensures appropriate decision rights to answer, **"Is the business doing enough?"**
- **Security & Risk Management** leaders typically own core security processes
- **Effectiveness** of the security program are monitored and communicated to business stakeholders

This is not a full set of processes and security services required for a mature security program; however, they demonstrate the foundations that must be in place.

Questions?