naphsis | IDENTITY & SECURITY CONFERENCE

December 1-2 Gaylord National Harbor

That's a Rap on Security Compliance Frameworks

Tuesday December 2, 2025 | Gary Nelson, Principal – Schellman Compliance schellman

That’s a Rap on Compliance Assessments

Presenter

LinkedIn

Gary Nelson
Principal
Schellman

Husband of wife age 39+?; father of 3 ages 21, 18, and 16

Practice Leader in AICPA attestation services

Information security and privacy career spans over 25 years

Actively participate in multiple industry organizations, such as AICPA, ISACA, and CSA

Agenda

Three Popular Compliance Frameworks

- AICPA SOC
- ISO 27001
- NIST 800-53

AICPA SOC

But first…

AICPA SOC

SOC 1

- ***Who Needs It:*** Service Organizations that perform outsourced business processes
- ***Subject Matter:*** Internal Controls over Financial Reporting
- ***Scope:*** Control Objectives identified by the Service Organization
- ***Focus:*** ITGC and Completeness/Accuracy/Timeliness/Authorization of processes

SOC 2

- ***Who Needs It:*** Service Organizations that provide (X)aaS offerings
- ***Subject Matter:*** Service Commitments and AICPA Trust Services Criteria
- ***Scope:*** Subject Matter above identified by the Service Organization
- ***Focus:*** Security, Availability, Confidentiality, Processing Integrity, and Privacy

ISO 27001

But first…

ISO 27001

- ***Who Needs It:*** Organizations that typically have international clients or operations
- ***Subject Matter:*** Information Security Management System (ISMS)
- ***Scope:*** ISO 27001 Clauses and Annex A controls
- ***Focus:*** Governance, oversight, and management of security over processes

NIST 800-53

But first…

NIST 800-53

- ***Who Needs It:*** Organizations that typically perform services for the US government
- ***Subject Matter:*** NIST 800-53 Rev5
- ***Scope:*** 17 Families of Controls
- ***Focus:*** Security and privacy requirements defined by NIST

Summary Comparison

	AICPA SOC	ISO 27001	NIST 800-53
Who Needs It (typically)	SOC 1: Outsourced Business Process SOC 2: Outsourced (X)aaS	Companies with international locations or customers	Companies that perform services for government entities
Subject Matter	SOC 1: ICFR SOC 2: Service Commitments and AICPA TSC	ISMS	NIST 800-53 Rev5
Scope	SOC 1: Control Objectives SOC 2: Trust Services Categories	ISO 27001 Clauses and Annex A Controls	17 Control Families
Focus	SOC 1: ITGC and options for Completeness, Accuracy, Timeliness, Authorization of Business Processes SOC 2: Security Category and options of Availability, Confidentiality, Processing Integrity, and Privacy Categories	Governance, oversight, and management of security over processes	Security and privacy requirements defined by NIST

Assessment & Certification Examples

SOC EXAMINATIONS

SOC 1
SOC 2
SOC 3
SOC for Cybersecurity
SOC for Supply Chain
CSA STAR Attestation

ISO CERTIFICATIONS

ISO 9001
ISO 20000-1
ISO 22301
ISO 27001
ISO 27018
ISO 27701
CSA STAR Certification

FEDERAL ASSESSMENTS

FedRAMP / StateRAMP
CMMC
NIST 800-53 / FISMA
NIST 800-171
CJIS
ITAR
FTC Consent Decrees

PAYMENT CARD ASSESSMENTS

PCI DSS (4.0)
PCI P2PE
PCI 3DS
PCI PIN
Secure Software Framework

CYBERSECURITY ASSESSMENTS

NY DFS Assessment
NIST CSF Assessment
Crypto & Digital Trust
Software Security Assessment
Training & Certification Services

HEALTHCARE ASSESSMENTS

HITRUST
HIPAA
EPCS-DEA

CLOUD SECURITY

Penetration Testing
Social Engineering
Red Teaming
Physical Security
IoT & Hardware

INTERNAL AUDIT ASSESSMENTS

IT General Controls Testing
Business Process Control Testing
Internal Audit Co-Sourcing
SOX Internal Audit Support

PRIVACY PROGRAM ASSESSMENTS

APEC Certification
GDPR
MS DPR / SSPA Assessment
CCPA
US & International Laws

FINANCIAL ASSESSMENTS

SWIFT CSP
FFIEC
GLBA
Cybersecurity

INTERNATIONAL ASSESSMENTS

C5 Assessment
HDS
IRAP
TISAX Audit Provider
DORA

SUSTAINABILITY ASSESSMENTS

ESG Assessments
ESG Assurance
ESG Certification
GHG Assurance
ISO 14001

RISK MANAGEMENT ASSESSMENTS

Third Party Risk Assessments
Vendor Assessment Assistance
Private Equity (PE) Portfolio Review

ARTIFICIAL INTELLIGENCE

NIST AI RMF
ISO 42001
HITRUST + AI
Adversarial Machine Learning

Questions

?

Thank You

schellman

www.schellman.com

info@schellman.com

1.866.254.0000

Int’l +1.813.288.8833

Follow @Schellman on Social Media: