schellman

Panel Discussion: Compliance Assessments & Best Practices

Schellman, NAPHSIS, and OCISO

Presenters *(Schellman)*

Gary Nelson

Principal

Alexis Smith

Manager

Presenters *(NAPHSIS & OCISO)*

Alan Harbin

NAPHSIS

Michael Pruett

Office of the CISO

NAPHSIS Perspective

Question:

What were the factors that led you to utilizing external consultants to lead your compliance assessments instead of in-house personnel?

OCISO Perspective

Question:

What is one of the first things you communicate to a client that is engaging you for leading compliance efforts and assessments?

Schellman Perspective

Question:

What goes into your planning to perform an assessment when a consultant is assisting your client that needs the assessment?

All Panelists

Discussion Points:

- Pitfalls and challenges encountered in these projects
- Paths taken to overcome those challenges

All Panelists

Discussion Points:

- Best practices for project management and scheduling during an assessment
- Impact of adding more compliance initiatives on efforts

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

Future Considerations (AI)

Bonus Question:

Has AI been more of a benefit or concern for any of your efforts?

Questions

Thank You

www.schellman.com

info@schellman.com

1.866.254.0000

Int'l +1.813.288.8833

Follow @Schellman on Social Media: