HITRUST Users Group

SOC 2 vs. HITRUST

SureIT

Quick Comparison

HITRUST Assessment	SOC 2 Type 2 Audit
Accredited by HITRUST Alliance	Accredited by AICPA
Point in Time	Specified Date Range
Controls must be implemented at least 90 days prior to assessment date	Controls must be implemented during the audit period
Conducted by external assessor and QA reviewed by HITRUST Alliance	Conducted by external auditor, but not reviewed by AICPA
Prescriptive - very specific control language and guidance	Trust Principles – more discretion of controls to implement

SureIT

Evidence Overlap

- Policies and Standards
- People Team Procedures
  - Onboarding
  - Sanctions/Discipline
  - Training & Certifications
  - Termination
- Information Protection/Security Program
  - Risk Management
  - Third Party Assurance
  - Governance
  - Incident Response

SureIT

Which One to Choose?

- HITRUST or SOC 2
  - Depends on your org preferences and/or client requirements
  - HITRUST for prescriptive controls if you are starting with little or no established governance
  - SOC 2 if you have established security controls or if you have Trust Principle requirements outside the HITRUST controls (e.g. Processing Integrity)
- HITRUST and SOC 2
  - The scope of each must be the same
  - Must include SOC 2 Security, Availability and Confidentiality Trust Principles
- HITRUST with SOC 2
  - Allows flexibility in scoping each assessment/audit
  - Reliance on one to assist with the other – no need to gather evidence twice

SureIT