5.2

Monday, October 2, 2023 5:11 PM

PCI DSS

12 reqs aimed to ensure orgs maintain secure env

- encrypt
- use firewall
- restrict data
- maintain access logs

Center for Internet Security CIS

20 CIS controls

Risk assessment Method CIS-RAM

overall evaluation of sec posture

Configuration access tool CIS-CAT

Configuration access tool CLS-CAT

used w/ auto vuln scanners

to test compliance against

benchmarks

Security technical implementation

guides STIGs + hardening

guides for variety of soft/hard

solutions

National checklist program NCP -

checklists and benchmarks

for OS and apps

CSA - Cloud sec alliance

provides resources to assist CSP

& deliver services

provide ...

in setting up & deliver services

Cloud controls matrix CSA-CCM - starting point for contracts / agree baseline sec competency

Enterprise reference architecture - best practice method/ tools for CSP to use in architect cloud solutions

security guidance - best prac summary and unique challenges of cloud env and how on-premises controls can be adapted

... attestation Engagements

Statements for attestation Engagements

SSAE - audit specs developed by American institute of cert public accountants AICPA

GDPR protection and accountability principles

- purpose limitation - orgs must process data that was collected for explicit purposes specified to data subject
- integrity and confidentiality
- data minimization - only collect and process as much data as

needed

does not specify where orgs store data only how and why

ISO 27001 - best practice spec for an info system (people, process, tech)

ISO 27002 - Standard focus on info sec controls that orgs may choose to implement

ISO 27701 - reqs and guidance for establish, implement, maintain, and continually improve an info system w/ private data