ControlCase

ENS
Innovate. Protect. Deliver

AUDIT CHECKLIST FOR REMOTE ZERO TRUST ENVIRONMENTS

Zero Trust Principles can be used to manage compliance with regulations including PCI DSS, ISO 27001, SOC 2 Type 2, GDPR, CCPA and FedRAMP.

DOMAIN 1: POLICY MANAGEMENT

- ☐ Provide Information Security Awareness Training to WFH users on how to secure their wireless network (if any).
- ☐ Are IT security policies updated?
- ☐ Does your user understand acceptable usage policy?
- ☐ Is access control policy in place emphasizing need to know basis access control?

DOMAIN 2: CONFIGURATION MANAGEMENT

- ☐ System configuration standards approved by organizations must be enforced on WFH users' workstations.
- ☐ Maintain the inventory of workstations.
- ☐ Are end user workstations enabled with personal firewall with minimum required connections allowed and deny everything else inbound/outbound?

DOMAIN 3: VULNERABILITY MANAGEMENT

- ☐ Internal vulnerability assessment and penetration testing must be conducted for WFH workstations.
- ☐ Penetration tests emulating a work from home user scenario must be performed.
- ☐ Do developers/programmers write secure code?

DOMAIN 4: LOG MANAGEMENT

- ☐ Ensure all user activities done on WFH workstations are logged.
- ☐ Ensure all WFH workstations are synchronizing time with designated NTP server.

DOMAIN 5: DATA MANAGEMENT

- ☐ Increase the frequency of PII data discovery scanning.
- ☐ Establish process to run automated secure data disposal on disks of workstations for WFH users.
- ☐ Reduce the exposure of PII
- ☐ Do database admins understand dataflows?

DOMAIN 6: PHYSICAL SECURITY

- ☐ Ensure controls (such as Citrix) are in place that full sensitive/PII data cannot be viewed or downloaded when working from home.
- ☐ Complete Data Center reviews.
- ☐ Reduce the exposure of PII.
- ☐ Is your physical equipment locked with double security, i.e., door, fence, cabinet, etc.?

AUDIT CHECKLIST FOR REMOTE ZERO TRUST ENVIRONMENTS

DOMAIN 7: ANTIVIRUS & ANTIMALWARE

- ☐ All systems should have an Anti-Virus solution installed and regularly updated.
- ☐ Users should not be able to disable the Anti-Virus solution.

DOMAIN 8: ACCESS MANAGEMENT

- ☐ No regular user (except power users) should be able to access any system that stores, processes or transmits sensitive/PII.
- ☐ All the WFH users must use two-factor authentication to connect to sensitive/PII environment.
- ☐ Need-to-know basis access along with least privileges must be implemented to restrict access to sensitive/PII data for WFH users.
- ☐ Is multi-factor authentication enabled for all users?

ABOUT CONTROLCASE:

ControlCase is a global provider of certification, cyber security and continuous compliance services. ControlCase is committed to empowering organizations to develop and deploy strategic information security and compliance programs that are simplified, cost effective and comprehensive in both on-premise and cloud environments. ControlCase offers certifications and a broad spectrum of cyber security services that meet the needs of companies required to certify to PCI DSS, HITRUST, SOC 2 Type II, ISO 27001, PCI PIN, PCI P2PE, PCI TSP, PCI SSF, CSA STAR, HIPAA, GDPR, SWIFT and FedRAMP.

YOUR IT COMPLIANCE PARTNER: Go beyond the auditor's checklist

Partnership Approach

Continuous Compliance Services

SkyCAM Platform for Automated Evidence Collection

For more information email contact@controlcase.com