



AUDIT CHECKLIST FOR MAINTAINING CONTINUOUS COMPLIANCE

ControlCase's Solution for making your IT compliance
"Business as Usual"



DOMAIN 1: POLICY MANAGEMENT

- ☐ Appropriate update of policies and procedures
- ☐ Link/Mapping to controls and standards
- ☐ Communication, training and attestation
- ☐ Monitoring of compliance to corporate policies

DOMAIN 2: VENDOR 3RD PARTY MANAGEMENT

- ☐ Management of third parties/vendors
- ☐ Self attestation by third parties/vendors
- ☐ Remediation Tracking

DOMAIN 3: ASSET VULNERABILITY MANAGEMENT

- ☐ Asset List
- ☐ Management of vulnerabilities and dispositions
- ☐ Training to development and support staff
- ☐ Management reporting if unmitigated vulnerability
- ☐ Linkage to non-compliance

DOMAIN 4: LOGGING AND MONITORING

- ☐ Logging
- ☐ File Integrity Monitoring
- ☐ 24X7 Monitoring
- ☐ Managing volumes of data

DOMAIN 5: CHANGE MANAGEMENT

- ☐ Logging and Monitoring (SEIM/FIM, etc.)
- ☐ Change management ticketing system
- ☐ Correlation of logs / alerts to change requests
- ☐ Response / Resolution process for expected logs / alerts
- ☐ Escalation to incident for unexpected logs / alerts

DOMAIN 6: INCIDENT / PROBLEM MANAGEMENT

- ☐ Monitoring
- ☐ Detection
- ☐ Reporting
- ☐ Responding
- ☐ Approving

MAINTAINING CONTINUOUS COMPLIANCE



DOMAIN 7: DATA MANAGEMENT

- ☐ Identification of data
- ☐ Classification of data
- ☐ Protection of data
- ☐ Monitoring of data

DOMAIN 8: RISK MANAGEMENT

- ☐ Input of key criterion
- ☐ Numeric algorithms to compute risk
- ☐ Output of risk dashboards

DOMAIN 9: BUSINESS CONTINUITY MANAGEMENT

- ☐ Business Continuity Planning
- ☐ Disaster Recovery
- ☐ BCP / DR Testing
- ☐ Remote Site / Hot Site

DOMAIN 10: HR MANAGEMENT

- ☐ Training
- ☐ Background Screening
- ☐ Reference Checks

DOMAIN 11: PHYSICAL SECURITY

- ☐ Badges
- ☐ Visitor Access
- ☐ CCTV
- ☐ Biometric

ControlCase Testing Automation

