IT Best Practices Audit™

TCS offers a wide range of IT Best Practices Audit content covering 15 subjects and over 2200 topics, including:

1. IT Cost Containment — 84 topics
2. Cloud Computing Readiness — 225 topics
3. Networks — 185 topics
4. Desktops and Printers — 208 topics
5. Storage — 130 topics
6. Microsoft Servers — 191 topics
7. iSeries Servers — 116 topics
8. Web Servers — 119 topics
9. Unix and Linux Servers — 134 topics
10. Database — 115 topics
11. Software Licensing — 24 topics
12. Telephony — 82 topics
13. Data Center — 253 topics
14. IT Leadership and Governance — 185 topics
15. Compliance and Security — 296 topics

Compliance and Security Audit Categories and Topics

Category	Audit Topic
General/Info	Name(s) of client resources providing data for this subject
General/Info	Title(s) of client resources providing data for this subject
Cost Metrics	IT Cost Metrics - Total Annual per device Cost for Compliance and Security related functions (Total costs / number of supported IT devices)
Cost Metrics	IT Cost Metrics - Number of devices supported per Compliance and Security Support Staff FTE
Information Security	Information security program
Information Security	Management oversight and approval
Information Security	Information security program reporting
Information Security	Adjustment of the information security program
Information Security	Information security policy
Information Security	Information security policy document
Information Security	Review of the information security policy
Information Security	Review of the information security policy document
Organization of Information Security	Internal organization
Organization of Information Security	Management commitment to information security
Organization of Information Security	Information security co-ordination
Organization of Information Security	Allocation of information security responsibilities
Organization of Information Security	Information security officer
Organization of Information Security	Security alerts management
Organization of Information Security	Security incident management
Organization of Information Security	User administration
Organization of Information Security	Data access management
Organization of Information Security	Authorization process for information processing facilities
Organization of Information Security	Confidentiality agreements
Organization of Information Security	Contact with authorities
Organization of Information Security	Contact with special interest groups
Organization of Information Security	Independent review of information security
Organization of Information Security	External parties

Category	Audit Topic
Organization of Information Security	Identification of Risks related to external third parties
Organization of Information Security	Protection of hosted environment
Organization of Information Security	Management of connected entities
Organization of Information Security	Addressing security when dealing with customers
Organization of Information Security	Addressing security in third party agreements
Organization of Information Security	Documentation of 3rd party assurances
Organization of Information Security	Third party information use and disclosure
Organization of Information Security	Third party reporting of security incidents
Organization of Information Security	Termination of third party agreements
Organization of Information Security	Third party regulatory compliance
Asset Management	Responsibility for assets
Asset Management	Inventory of assets
Asset Management	Ownership of assets
Asset Management	Acceptable use of assets
Asset Management	Acceptable use of workstations
Asset Management	Acceptable use of technology
Asset Management	Maintenance of access list
Asset Management	Acceptance secure usage
Asset Management	Information classification
Asset Management	Classification guidelines
Asset Management	Information labeling and handling
Human Resources Security	Prior to employment
Human Resources Security	Roles and responsibilities
Human Resources Security	Screening
Human Resources Security	Terms and conditions of employment
Human Resources Security	During employment
Human Resources Security	Management responsibilities
Human Resources Security	Information security awareness, education, and training
Human Resources Security	Information security awareness
Human Resources Security	Information security education and training
Human Resources Security	Disciplinary process
Human Resources Security	Termination or change of employment

Category	Audit Topic
Human Resources Security	Termination responsibilities
Human Resources Security	Return of assets
Human Resources Security	Removal of access rights
Physical and Environmental Security	Secure areas
Physical and Environmental Security	Physical security policies and procedures
Physical and Environmental Security	Physical security maintenance records
Physical and Environmental Security	Physical security perimeter
Physical and Environmental Security	Physical entry controls
Physical and Environmental Security	Identification badges
Physical and Environmental Security	Visitor access control
Physical and Environmental Security	Securing offices, rooms, and facilities
Physical and Environmental Security	Securing workstations
Physical and Environmental Security	Securing network jacks
Physical and Environmental Security	Securing wireless access points
Physical and Environmental Security	Protecting against external and environment threats
Physical and Environmental Security	Working in secure areas
Physical and Environmental Security	Surveillance
Physical and Environmental Security	Retention of surveillance data
Physical and Environmental Security	Security of field offices
Physical and Environmental Security	Public access, delivery, and loading areas
Physical and Environmental Security	Equipment security
Physical and Environmental Security	Equipment siting and protection
Physical and Environmental Security	Supporting utilities
Physical and Environmental Security	Cabling security
Physical and Environmental Security	Equipment maintenance
Physical and Environmental Security	Security of equipment off-premises
Physical and Environmental Security	Secure disposal or re-use of equipment
Physical and Environmental Security	Removal of property
Communications and Operations Management	Operational procedures and responsibilities
Communications and Operations Management	Documented operating procedures
Communications and Operations Management	Change management
Communications and Operations Management	System update and patch process

Category	Audit Topic
Communications and Operations Management	Segregation of duties
Communications and Operations Management	Separation of development, test, and operational facilities
Communications and Operations Management	Monitoring
Communications and Operations Management	Audit logging
Communications and Operations Management	Automated audit trails
Communications and Operations Management	Audit events
Communications and Operations Management	Retention of audit trails
Communications and Operations Management	Monitoring system use
Communications and Operations Management	Monitoring system access
Communications and Operations Management	Protection of log information
Communications and Operations Management	Limit access to audit trails
Communications and Operations Management	Backup of audit trails
Communications and Operations Management	Wireless network logs
Communications and Operations Management	Protecting integrity of audit trail
Communications and Operations Management	Administrator and operator logs
Communications and Operations Management	Fault logging
Communications and Operations Management	Clock synchronization
Communications and Operations Management	Data retention
Communications and Operations Management	Third-party service delivery management
Communications and Operations Management	Service delivery
Communications and Operations Management	Monitoring and review of third-party services
Communications and Operations Management	Managing changes to third-party services
Communications and Operations Management	System planning and acceptance
Communications and Operations Management	Capacity management
Communications and Operations Management	Baseline security configuration
Communications and Operations Management	Segregation of servers
Communications and Operations Management	Disabling of unnecessary protocols, services, and functionality
Communications and Operations Management	System acceptance
Communications and Operations Management	Protection against malicious and mobile code
Communications and Operations Management	Controls against malicious code
Communications and Operations Management	Anti-virus safeguards
Communications and Operations Management	Safeguards against spyware and adware

Category	Audit Topic
Communications and Operations Management	Controls against mobile code
Communications and Operations Management	Back-up
Communications and Operations Management	Information backup
Communications and Operations Management	Network security management
Communications and Operations Management	Network controls
Communications and Operations Management	Direct access to information
Communications and Operations Management	Restrict outbound traffic
Communications and Operations Management	IP masquerading
Communications and Operations Management	Channel encryption
Communications and Operations Management	Encryption of administrative access
Communications and Operations Management	Encryption of data on wireless networks
Communications and Operations Management	Intrusion detection
Communications and Operations Management	Updates to intrusion detection and prevention systems
Communications and Operations Management	Proactive vulnerability scanning
Communications and Operations Management	Wireless network scanning
Communications and Operations Management	Penetration tests
Communications and Operations Management	Security of network services
Communications and Operations Management	Changes to default configuration
Communications and Operations Management	Media handling
Communications and Operations Management	Management of removable media
Communications and Operations Management	Removable media maintenance records
Communications and Operations Management	Management approval for movement of media
Communications and Operations Management	Reuse of media
Communications and Operations Management	Disposal of media
Communications and Operations Management	Destruction of hardcopy materials
Communications and Operations Management	Destruction of electronic media
Communications and Operations Management	Information handling procedures
Communications and Operations Management	Inventory of removable media
Communications and Operations Management	Protection of sensitive authentication data
Communications and Operations Management	Security of system documentation
Communications and Operations Management	Exchange of information
Communications and Operations Management	Information exchange policies and procedures

Category	Audit Topic
Communications and Operations Management	Exchange agreements
Communications and Operations Management	Physical media in transit
Communications and Operations Management	Transportation of media
Communications and Operations Management	Electronic messaging
Communications and Operations Management	Business information systems
Communications and Operations Management	Electronic commerce services
Communications and Operations Management	Electronic commerce
Communications and Operations Management	On-Line transactions
Communications and Operations Management	Publicly available information
Access Control	Business requirement for access control
Access Control	Access control policy
Access Control	User access management
Access Control	User registration
Access Control	Inactive user accounts
Access Control	Vendor accounts
Access Control	Privilege management
Access Control	Access management for terminated users
Access Control	Password management
Access Control	Review of user access rights
Access Control	User responsibilities
Access Control	Communication of password policies and procedures
Access Control	Password use
Access Control	Unattended user equipment
Access Control	Clear desk and clear screen policy
Access Control	Network access control
Access Control	Policy on use of network services
Access Control	User authentication for external connections
Access Control	Two-factor authentication
Access Control	Equipment identification in networks
Access Control	Remote port protection
Access Control	Segregation in networks
Access Control	Network connection control

Category	Audit Topic
Access Control	Firewalls
Access Control	Session timeout for modems or VPN connections
Access Control	Network routing control
Access Control	DMZ
Access Control	Operating system access control
Access Control	Secure log-on procedures
Access Control	User identification and authentication
Access Control	Password management system
Access Control	Use of system utilities
Access Control	Session time-out
Access Control	Limitation of connection time
Access Control	Application and information access control
Access Control	Information access restriction
Access Control	Sensitive system isolation
Access Control	Isolation of databases
Access Control	Mobile computing and teleworking
Access Control	Mobile computing and communications
Access Control	Teleworking
Information Systems Acquisition, Development, and Maintenance	Security requirements of information systems
Information Systems Acquisition, Development, and Maintenance	Security requirements analysis and specification
Information Systems Acquisition, Development, and Maintenance	Correct processing in applications
Information Systems Acquisition, Development, and Maintenance	Input data validation
Information Systems Acquisition, Development, and Maintenance	Control of internal processing
Information Systems Acquisition, Development, and Maintenance	Message integrity
Information Systems Acquisition, Development, and Maintenance	Output data validation
Information Systems Acquisition, Development, and Maintenance	Cryptographic controls

Category	Audit Topic
Information Systems Acquisition, Development, and Maintenance	Policy on the use of cryptographic controls
Information Systems Acquisition, Development, and Maintenance	Encryption
Information Systems Acquisition, Development, and Maintenance	Key management
Information Systems Acquisition, Development, and Maintenance	Protection of encryption keys
Information Systems Acquisition, Development, and Maintenance	Key management processes
Information Systems Acquisition, Development, and Maintenance	Protection of disk encryption keys
Information Systems Acquisition, Development, and Maintenance	Digital signatures
Information Systems Acquisition, Development, and Maintenance	Non-repudiation services
Information Systems Acquisition, Development, and Maintenance	Security of system files
Information Systems Acquisition, Development, and Maintenance	Control of operational software
Information Systems Acquisition, Development, and Maintenance	Changes to default configuration
Information Systems Acquisition, Development, and Maintenance	Testing of operational changes
Information Systems Acquisition, Development, and Maintenance	Control of operational code
Information Systems Acquisition, Development, and Maintenance	Protection of system test data
Information Systems Acquisition, Development, and Maintenance	Removal of test data from production systems
Information Systems Acquisition, Development, and Maintenance	Access control to program source code
Information Systems Acquisition, Development, and Maintenance	Integrity protection of system files
Information Systems Acquisition, Development, and Maintenance	Security in development and support processes
Information Systems Acquisition, Development, and Maintenance	Software development methodology and guidelines

Category	Audit Topic
Information Systems Acquisition, Development, and Maintenance	Secure design education
Information Systems Acquisition, Development, and Maintenance	Threat assessment
Information Systems Acquisition, Development, and Maintenance	Secure coding guidelines
Information Systems Acquisition, Development, and Maintenance	Security code review
Information Systems Acquisition, Development, and Maintenance	Security quality assurance
Information Systems Acquisition, Development, and Maintenance	Change control procedures
Information Systems Acquisition, Development, and Maintenance	Risk assessment for major changes
Information Systems Acquisition, Development, and Maintenance	Technical review of system changes
Information Systems Acquisition, Development, and Maintenance	Restrictions on changes to software packages
Information Systems Acquisition, Development, and Maintenance	Information leakage
Information Systems Acquisition, Development, and Maintenance	Outsourced software development
Information Systems Acquisition, Development, and Maintenance	Technical vulnerability management
Information Systems Acquisition, Development, and Maintenance	Control of technical vulnerabilities
Information Systems Acquisition, Development, and Maintenance	Vulnerability review of information systems
Information Security Incident Management	Reporting information security events and weaknesses
Information Security Incident Management	Reporting information security events
Information Security Incident Management	Reporting security weaknesses
Information Security Incident Management	Management of information security incidents and improvements
Information Security Incident Management	Incident management responsibilities and procedures
Information Security Incident Management	Testing of incident response plan
Information Security Incident Management	Alerts from monitoring systems
Information Security Incident Management	Allocation of responsibilities

Category	Audit Topic
Information Security Incident Management	Learning from information security incidents
Information Security Incident Management	Training for security breach responsibilities
Information Security Incident Management	Collection of evidence
Business Continuity Management	Information security aspects of business continuity management
Business Continuity Management	Including information security in the business continuity management process
Business Continuity Management	Business continuity and risk assessment
Business Continuity Management	Developing and implementing continuity plans including information security
Business Continuity Management	Disaster recovery plan
Business Continuity Management	Emergency mode operation plan
Business Continuity Management	Business continuity planning framework
Business Continuity Management	Testing, maintaining, and reassessing business continuity plans
Risk Management	Risk assessment review
Risk Management	Risk treatment/documented decisions
Compliance	Compliance with legal requirements
Compliance	Identification of applicable legislation
Compliance	Intellectual property rights (IPR)
Compliance	Protection of organizational records
Compliance	Data protection and privacy of personal information
Compliance	Masking of sensitive data
Compliance	Prevention of misuse of information processing facilities
Compliance	Regulation of cryptographic controls
Compliance	Compliance with security policies and standards, and technical compliance
Compliance	Compliance with security policies and standards
Compliance	Technical compliance checking
Compliance	Information systems audit considerations
Compliance	Information systems audit controls
Compliance	Protection of information systems audit tools
Compliance	Response to compliance findings
Compliance	Mechanisms for reporting compliance with legislation, standards and policies
Privacy	Privacy policy and procedures
Privacy	Privacy policy document
Privacy	Retention of privacy policy document

Category	Audit Topic
Privacy	Privacy roles and responsibilities
Privacy	Notices are designed and managed to comply with applicable laws, regulations and standards that may specify content, delivery, frequency, documentation, retention, and change requirements.
Privacy	Notices are designed to Inform individuals of the types of information collected, the intended uses of the information, and how that information is shared with third parties.
Privacy	Notices Include the options available to the individual including how to contact the organization with a privacy complaint or inquiry and the options available for limiting the use and disclosure of their personal information.
Privacy	Notices are provided in clear and conspicuous language and presented prior to the collection of personal information.
Privacy	Choice / consent
Privacy	Use and sharing of information
Privacy	Integrity of information
Privacy	Access to information
Privacy	Confidential communications