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

IT Best Practices Audit™

Networks 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
General/Info	Network topology documentation
General/Info	Documentation of how key applications use the network - when, where, how much, latency and bandwidth needs, etc.
General/info	Maximum theoretical bandwidth of LAN
General/info	Maximum theoretical bandwidth of WAN in Mb/s
General/info	Internet Link download and upload speeds in Mb/s
General/info	Inventory and map of devices by switch and port
General/info	Proactive meetings/communication with vendor representatives
General/info	Network Vendor(s)
General/Info	Vendor contact information
General/Info	Vendors have current client contact information
Cost Metrics	IT Cost Metrics - Total Annual Cost Per Network Port
Cost Metrics	IT Cost Metrics - Number of Network Ports supported per Network Support Staff FTE
Staffing	Network Staffing
Staffing	Network Staff training
Reliability	Overall Availability (% of planned uptime) of wired network
Reliability	Overall Availability (% of planned uptime) of wireless networks
Reliability	Hardware Failures (routers, firewalls, VPN appliances, load balancers, DNS servers, switches, etc.)
Reliability	Software Failures (of routers, load balancers, VPN, firewalls, DNS servers, switches, etc.)
Reliability	Circuit Failures (dial-up analog and digital, cable modems, DSL, T-1's, DS3's, Broadband/metro Ethernet, wireless, etc.) Private and shared circuits.
Reliability	Other failures (ISP related, hosting provider, trading partners, unknown)
Utilization	Network Traffic identified
Utilization	Average LAN latency for each link
Utilization	Average WAN latency for each link
Utilization	WAN - average circuit utilization during business hours
Utilization	Variability of traffic loads

Category	Audit Topic
Utilization	WAN - number of seconds per minute of 100% link utilization
Utilization	LAN - number of seconds of 100% link utilization per minute during "normal" business use/hours (not during backups, etc.)
Utilization	WAN capacity (relative to the size of the enterprise or locations being linked
Utilization	WAN reliability (average per link)
Utilization	Core Router CPU capacity and utilization
Utilization	Core Router memory/address table capacity and utilization
Utilization	Router and switch ports and capacity
Utilization	Core Router Actual Packets Per Second (PPS) forwarding rates vs. rated capacity, etc.
Utilization	Core Switch CPU capacity and utilization
Utilization	Core Switch memory/address table capacity and utilization
Utilization	Core Switch - Actual Packets Per Second (PPS) forwarding rates vs. rated capacity, etc.
Utilization	Total Daily error counts on all router ports
Utilization	Total Daily error counts on all switch ports
Utilization	Typical latency (Ping) to Google, Yahoo or other common access points
Utilization	Typical latency (Ping) to client or supplier web sites or other common access points
Utilization	Use of speed tests (www.Speedtest.net) to determine typical Internet throughput rates
Utilization	Perform pings and tracert's to each end point in the network – look for high latency, variable latency, dropped packets, number of hops, identify any changes
Utilization	Core Router port utilization
Utilization	Remote LAN Closets - uplink capacity
Utilization	Remote LAN Closets - uplink utilization
Operations	Network Traffic monitoring performed
Operations	Use hardware diagnostics to check on health of NIC – retransmits, etc.
Operations	Use MS Net Watcher 3.0, Ethereal, or Wireshark type packet sniffer to look at network
Operations	Ownership of wireless access points
Operations	Network Security and Monitoring
Operations	Monitor performance of the switches and routers – memory utilization, CPU utilization, error counts
Operations	Wiring closets and uplinks
Operations	Send alarms (IM's/emails/pages) for high ping times from remote sites
Operations	Discussions/status meetings with key integrated partners and/or customers (shared web sites, file transfers, use of SaaS apps, API's, etc.) on the state of the communications links that connect them to the organization.

Category	Audit Topic
Operations	Reporting of key network based tasks
Operations	Advance notification of planned changes
Operations	Configuration backups
Operations	Network Disaster Recovery plan
Operations	24 x 7 monitoring of network health
Operations	Use of Wireless Bridges to connect Ethernet devices - printers, etc
Operations	Maintenance Windows
Hardware	Dedicated Network Test environment
Hardware	Network cable plant
Hardware	Certification and testing of Fiber Optic cables
Hardware	UPS protection
Hardware	Use of Power Conditioning and Surge Protectors
Hardware	Cost of downtime
Hardware	% of network equipment 25 - 48 months old
Hardware	% of network equipment less than 24 months old
Hardware	% of network equipment more than 48 months old
Hardware	Network Tools (software) owned and used
Hardware	Network Tools (hardware) owned and used
hardware	Use of non-Ethernet components for PC's and Server interconnects
hardware	Use of non CAT 5/6 type cable
Hardware	Class of Ethernet switches in use
Hardware	Spare network related equipment (cables, routers, switches, etc.)
Hardware	Use of Power over Ethernet (POE) switches
Hardware	Use of standardized equipment/components
Configuration	WAN media
Configuration	WAN backup
Configuration	WAN link protocol
Configuration	WAN Routing Protocol
Configuration	Network Traffic prioritization
Configuration	TCP/IP tuning - ACK, Max frame size, etc. for Server 2003 and XP or older
Configuration	Maximum Transmit Unit (MTU) size
Configuration	TCP1323OPTS = 1 to allow window sizes greater than 65K bytes

Category	Audit Topic
Configuration	TCPWINDOWSIZE=65K for 100Mbs links – more for 1GB
Configuration	TCPACKFREQUENCY parameter
Configuration	Firewalls
Configuration	Tuning of Router configurations
Configuration	Patching of data comm software
Configuration	Separate network for print traffic
Configuration	Separate physical network for Latency sensitive traffic (Terminal Servers, Citrix, VDI)
Configuration	Separate network for data traffic - databases, iSCSI, NAS type traffic
Configuration	Separate network for web traffic
Configuration	Separate network for e-commerce traffic
Configuration	Separate network for backup traffic
Configuration	Separate network for network management traffic
Configuration	Separate network for VOIP traffic
Configuration	Use of dedicated network links/bandwidth (T-1, metro or long distance Ethernet, etc) vs. shared networks (Internet, MPLS, etc.) to minimize latency and number of hops
Configuration	Router/throughput limits
Configuration	Ethernet configuration rules
Configuration	Use IPv6 in the network
Wireless Configuration and security	Wireless access point speed
Wireless Configuration and security	Wireless access point encryption security in use
Wireless Configuration and security	Determination of wireless access point locations and required coverage
Wireless Configuration and security	Antenna selection for wireless access points
Wireless Configuration and security	Scanning for rogue wireless access points
Wireless Configuration and security	Physical security of wireless access points
Wireless Configuration and security	Use of IPSec-based Virtual Private Network (VPN) technology for end-to-end security between devices
Wireless Configuration and security	Use of 802.1x-based authentication to control access to the network
Wireless Configuration and security	Is the wireless network on a separate VLAN?
Wireless Configuration and security	Is firmware up-to-date in client cards and access points?
Wireless Configuration and security	Ability to reset the access points
Wireless Configuration and security	Disabling of access points during non-usage periods
Wireless Configuration and security	Password strength of access points
Wireless Configuration and security	Broadcasting of network SSIDs

Category	Audit Topic
Wireless Configuration and security	Propagation of radio waves outside the facility
Wireless Configuration and security	Use of personal firewalls
Wireless Configuration and security	Deployment of wireless LANs policy
Configuration	Use of secure device passwords
Configuration	Use of Encrypted Ethernet
Configuration	Telecommuter Policy
Configuration	Telecommuter Support
Configuration	Use of secure VPN for remote workers
Configuration	VPN client configuration (antivirus levels, etc.) validated prior to allowing connection
Configuration	Use of single sign-on
Configuration	Use of backup WAN links to carry normal traffic in an active/active load sharing configuration
Configuration	Use of backup WAN links to segment lower priority traffic
Configuration	Typical PC uplink speeds
Configuration	Typical speeds for network links to Servers
Configuration	Are PC uplink speeds at the maximum rate of the NIC - for example, a 1000 speed NIC is attached to a 1000 speed port
Configuration	Switch interconnects
Configuration	Use of Switch Ports
Configuration	Configuration of key devices (full/half, auto, etc.)
Configuration	Hardware to support LAN subnets
Configuration	Use of DHCP to manage TCP/IP addresses
Configuration	DHCP Lease length
Configuration	Device naming conventions
Configuration	Hardcoded IP addresses
Configuration	Overlap of DHCP and hard coded IP addresses
Configuration	Subnets used/ sizes
Configuration	Firmware levels / patch levels
Configuration	TCP/IP offload capabilities of NIC utilized
Configuration	NIC Load balancing
Configuration	NIC parameter tuning
Configuration	BizTalk capacity limits
Configuration	Ethernet switch nesting

Category	Audit Topic
Configuration	Use of Windows Advanced Server 2003 (or greater) NLB (Network Load Balance) Service
Configuration	Voice over Internet Protocol used
Configuration	Throttling of traffic by middleware
Configuration	ISP Assessment
Configuration	Hosting provider ISP interconnects
Configuration	Identification of key ISP's/likely routes for key customer traffic
Configuration	Use of Load balancing across multiple web servers for internet traffic
Configuration	Use of Hot Standby Routers for Internet traffic
Configuration	DNS servers/services
Configuration	Use of Border Gateway Protocol V4 to provide redundant IP access to multiple ISP's
Configuration	Use of multiple ISP's to provide Internet redundancy
Configuration	Migration from S2003/XP or earlier to S2008/Vista/W7 - changes in TCP/IP tuning can increase throughput and peak loads on networks
Security	Regular security audits
Security	Use of 3rd party penetration testing
Security	Use of Security Experts
Security	Use of Intrusion Detection
Security	Use of Intrusion Prevention
Security	Use of White-lists
Security	Server hardening
Security	Use of dial In circuits (or other circuits that bypass network security) by IT staff or vendors/consultants to access internal systems
Security	Use of LDAP or Active Directory and Group Policies for central control of most device/network security/access control
Security	Validation of authorized LDAP or Active Directory users and access rights/Group Policies against lists of current and authorized employees and vendors
Security	Virtualization Security
Security	Use of commercial quality firewalls - Cisco, Juniper, Checkpoint, Sonicwall, Barracuda, Nortel, etc.)
Security	Use of commercial quality VPNs - Cisco, Barracuda, Juniper, Checkpoint, Sonicwall, Nortel, etc.)
Security	Continuous Traffic Cleansing and monitoring
Security	Use of Router to Router VPN tunnels to connect multiple sites
Security	IP Filtering/controls to restrict bandwidth utilization/restrict access to non-business sites (no ESPN for example).

Category	Audit Topic
Security	Use of subnets and network segmentation to prohibit access to key components from most client or public machines
Security	Application Controls
Security	Log Inspection
Application Development Security	Development of secure applications
Application Development Security	Securing existing applications
Application Development Security	Use of security scanning tools
Application Development Security	Training for developers on how to develop secure applications