ISO 27001 Router Security Audit Checklist

Questions	Findings Yes	Findings No	ISO 27001 Control	Standard/Best Practice
Router Policy				
Is a router security policy in place?			A.5.1.1 A.11.4.1	
Disable Unneeded Services				
Are unused interfaces disabled?			A.11.4.4	Unused interfaces on the router should be disabled. Router(config-if)# shutdown
Is DNS lookups for the router turned off?			A.11.5.4 A.12.6.1	This client service is enabled by default and is not required on most routers. The following command is used to turn DNS lookup off. Router(config)#no ip domain-lookup
Is TCP small servers and UDP small servers service disabled on the router? {applicable before Cisco IOS 11.3}			A.12.6.1	These services are rarely used and hence can be disabled. This is disabled by default after Cisco IOS 11.3 Router(config)#no service tcp-small-servers Router(config)#no service udp-small-servers
Is Cisco Discovery Protocol disabled on the router?			A.11.4.4 A.12.6.1.	CDP which is used to obtain information such as the ip address, platform type of the neighboring Cisco devices should be disabled on the router if not used by any application. Router(config)# no cdp run OR Router(config-if)# no cdp enable
Is the finger service disabled on the router? {applicable before Cisco IOS 11.3}			A.11.4.4 A.11.5.4 A.12.6.1	Unauthorized persons can use the information obtained through this command for reconnaissance attacks. This service should be disabled. *Router(config)#no service finger*
Is Bootp server disabled on the routers?			A.11.4.4 A.11.5.4 A.12.6.1	The Bootp server service which is enabled by default allows other routers to boot from this router. This feature should be disabled on the router as it is rarely used on today's networks. The following command is used to disable the service. Router(config)#no ip bootp server
Is directed broadcast disabled on all interfaces? {applicable before Cisco IOS 11.3}			A.12.6.1	Directed broadcasts permit a host on one LAN segment to initiate a physical broadcast on a different LAN segment. This feature should be disabled on the router as it could be used in denial-of-service attacks. The following command is used to disable the service. Router(config-if)#no ip directed-broadcast
Is source routing disabled on the router?			A.12.6.1	Source routing is a feature that allows individual packets to specify routes. This is used in various attacks. This feature should be disabled on the router. The following command is used to disable the service. *Router(config)#no ip source-route*
Is Proxy ARP disabled on the router?			A.12.6.1	Proxy ARP helps in extending a LAN at layer 2 across multiple segments thereby breaking the LAN security perimeter. This feature should be disabled on the router. The following command is used to disable the service on individual interfaces. *Router(config-if)#no ip proxy-arp*
Is ICMP redirects disabled on the router?			A.12.6.1	The three ICMP messages that are commonly used by attackers for network mapping and diagnosis are: Host unreachable, 'Redirect' and 'Mask Reply'. Automatic generation of these messages should be disabled on all interfaces, especially those connected to untrusted networks. The following command is used to disable the service. *Router(config-if)#no ip redirects* *Router(config-if)#no ip unreachables* *Router(config-if)#no ip-mask reply*
Password Encryption				
Do passwords appear in encrypted form when viewed at the configuration file?			A.11.5.3	Passwords should appear encrypted when viewed through the configuration file. The following command is used to implement the same. *Router(config)#service password-encryption*
Authentication Settings				
Is enable secret used for the router enable mode?			A.11.5.3	The enable secret command should be enabled to implement MD5 hashed password on enable mode. *Router(config)#enable secret password*

source: http://www.TajDini.net

Does the enable secret password match any other username password; enable password, or the enable secret password of another router in the network?			A.11.5.3	The enable secret password should be unique across each router. If the routers are too many, instead of keeping a single enable secret password for all, the password could be different for routers in different zones.
Is a Message of the Day (MOTD) banner defined?			A.11.5.1	Login banners should be used as a preventive measure against unauthorized access to the routers. Use the following command to enable a MOTD banner: Router# config t Router(config)# banner motd ^
Is the following defined on the console port: 1. Exec-timeout 2. Password			A.11.5.1 A.11.3.1	These parameters should be defined on the console port to reduce the chance of an unauthorized access on the console port. The following commands can be used to implement the same: *Cisco(config)#line con 0* *Cisco(config-line)#exec-timeout 5 0* *Cisco(config-line)#password password* *Cisco(config-line)#login*
Is the aux port disabled?			A.11.4.4	The aux port should be disabled if there is no business need for the same. Use the following command to disable the aux port: *Router(config)#line aux 0* *Router(config-line)#no exec*
Is the following defined on the vty lines: 1. Exec-timeout (Yes/No) 2. Password			A.11.5.1 A.11.3.1	These parameter should be defined on the vty port to reduce the chance of an unauthorized access. Use the following to enable these parameters on the vty lines: Router(config)#line vty 0 4 Router(config-line)#exec timeout 5 0 Router(config-line)#password *password* Router(config-line)#login Router(config-line)#transport input *protocol*
Is the vty lines restricted to certain IP Addresses only?			A.11.4.3	If the vty lines use telnet as the transport protocol, it is advisable to restrict access to certain IP Addresses only since telnet transmits data in clear text. Use the following command to restrict vty access to certain ip addresses: Router(config)#access-list 50 permit 192.168.1.x (x represents the IP address of the administrator's machine) Router(config)#access-list 50 deny any log Router(config)#line vty 0 4 Router(config-line)#access-class 50 in
According to policy, how often do router passwords (telnet, username, enable) have to be changed?			A.11.5.3	Router passwords need to be changed periodically, typically once every 4-6 months depending on the functionality of the router.
Do the router passwords meet with the required complexity as defined by the policy?			A.11.3.1	All password defined on the router should meet the following criteria: · Minimum 8 characters in length · Should be alphanumeric along with special characters (@#$%) · Should not include organization's name in it
Is SSH used for the vty lines?			A.12.3.1	SSH is a preferred protocol over Telnet for vty access since it encrypts the data while in transit on the network.
Do any applications use telnet to perform management activities such as backing up configuration?			A.10.6.1	The Telnet protocol transfers data in clear text thereby allowing an intruder to sniff valuable data such as passwords. As a remedy the following can be done: · Using secure protocols such as SSH wherever possible · Restricting access from certain workstations only · Maintaining strong passwords
Administrator Authentication				
Is authentication on the router done through: · Locally configured usernames and passwords · TACACS+/RADUIS server				
Is there a documented procedure for creation of users?			A.10.1.1 A.11.2.1	A documented procedure for creation of administrators on the router should exist. The procedure should address: · Approval from the department head · Recording the authorization level given to the new administrator and the duration

source: http://www.TajDini.net

Does each router administrator have a unique account for himself/herself?			A.11.2.1	Each router administrator should have a unique account for him/her to maintain accountability. The following commands can be executed to create unique local usernames on the router: *Router(config)#**username** username **password** password* *Router(config)#line vty 0 4* *Router(config-line)#login local*
Is login and logout tracking/command logging for the router administrators through the TACACS+ system enabled?			A.10.10.1 A.10.10.4	A detailed log of every command typed on the router as well as when an administrator logged in or out can be recorded for audit purposes. Router(config)#aaa accounting exec default start-stop group tacacs+ Router(config)aaa accounting commands 15 default start-stop group tacacs+
Are all user accounts assigned the lowest privilege level that allows them to perform their duties? (Principle of Least Privilege)			A.11.2.2	All user accounts should be assigned the lowest privilege level that allows them to perform their duties. If multiple administrators exist on the router, each administrator should be given an individual username and password and assigned the lowest privilege levels.
Management Access				
Is the http/https Server used for router management?			A.10.6.1	This service allows the router to be monitored or have its configuration modified from the web browser. If not used, this service should be disabled. Router(config)#no ip http server If this service is required, restrict access to the http/https service using access control lists. Router(config)#ip http access-class 22 Router(config)#access-list 22 permit host *mgmt ip* Router(config)#access-list 22 deny any log
Which version of SNMP is used to manage the router?			A.10.6.1	Ideally SNMP version 3 should be used on the router since it introduces authentication in the form of a username and password and offers encryption as well. Since the SNMP process is enabled by default, it should be disabled if not used. Router(config)# no snmp-server
Is the SNMP process restricted to certain range of IP Addresses only?			A.10.6.1 A.11.4.3	If SNMP v1 or v2c is used, ACL's should be configured to limit the addresses that can send SNMP commands to the device. SNMP v1 or v2c uses the community string as the only form of authentication and is sent in clear text across the network. Router(config)#access-list 67 permit host *snmp-server* Router(config)#access-list 67 deny any log
Is the default community strings such as 'public' and 'private' changed?			A.11.2.3	Default community strings such as 'public' and 'private' should be changed immediately before bring the router on the network.
How often is the SNMP community string changed?			A.11.3.1	If SNMP v1 or v2c is being used, the SNMP community strings should be treated like root passwords by changing them often and introducing complexity in them.
Is any access list defined restricting the syslog host to receive log messages from the routers only and only administrators' systems to connect to the log host?			A.11.4.6	
Is the NTP server service used to synchronize the clocks of all the routers?			A.10.10.6	The NTP service which is disabled by default helps to synchronize clocks between networking devices thereby maintaining a consistent time which is essential for diagnostic and security alerts and log data. However if configured insecurely, it could used to corrupt the time clock of the network devices. To prevent this, restrict which devices have access to NTP. The service should also be disabled if not used.
Ingress/Egress Filtering				
				RFC 1918 addresses are meant to be used for internal networks only and have no reason to be seen on the Internet. The following access-lists should be implemented on the Internet router: Router(config)#access-list 101 deny ip 10.0.0.0 0.255.255.255 any log Router(config)#access-list 101 deny ip 172.16.0.0 0.15.255.255 any log Router(config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 any log

source: http://www.TajDini.net

Is RFC 1918 filtering implemented?			A.11.4.7	Router(config)#access-list 101 permit ip any any
Is uRPF enabled on the Cisco router?			A.11.4.7	Unicast Reverse Path Forwarding is an alternative to RFC 2827 filtering. It can enabled using the following commands: Router(config-if)#ip verify unicast reverse-path
Route Protocol Security				
Is routing protocol message authentication enabled?			A.11.4.7	Message authentication helps prevent the spoofing or modification of a valid routing protocol message.
Configuration Maintenance				
How often is the router configurations backed up?			A.10.5.1	Router configurations should be backed up periodically depending on importance and frequency of changes
Is the backup moved to an off-site/DR site?			A.10.5.1	Backup copies should be maintained off-site for quick recovery during a disaster.
On the system where the configuration files are stored, is the local operating system's security mechanisms used for restricting access to the files (i.e., the machine should be password enabled and prevent unauthorized individuals from accessing the machine.)?			A.10.5.1	If a file server is used to store configuration files, the files should be restricted to authorized personnel only.
Is the TFTP protocol used to transfer configuration or image files to and from the router? If yes, · Is the TFTP process restricted to certain addresses only? · Is the TFTP service disabled when not in use?			A.10.6.1	The TFTP protocol which is disabled by default transfers files in clear text and hence is unsafe to use. The TFTP process should be restricted to certain addresses only (management workstations) to reduce the risk. The service should also be disabled when not in use because it allows access to certain files in the router flash.
Is there a documented procedure for backup of router configurations?			A.10.5.1	
Router Change Management				
Are all router changes and updates documented in a manner suitable for review according to a change management procedure?			A.10.1.2	
Router Redundancy				
Is there a router redundancy in cold standby or hot standby?			A.14.1.3	
Are disaster recovery procedures for the router/network documented and are they tested?			A.14.1.3 A.14.1.5	
Log monitoring and Incident Handling				
Are all attempts to any port, protocol, or service that is denied logged?			A.13.1.1	
Is the CPU utilization/memory of the router monitored?			A.10.10.2	
Is logging to a syslog server enabled on the router?			A.10.10.1 A.13.1.1	Syslog messages allows for easy troubleshooting of the network. Use the following commands to enable syslog Router(config)#logging *syslog-ip-address* Router(config)#service timestamps log datetime localtime msec show-timezone
Are procedures for audit log review generated by the router documented and followed?			A.10.1.1	
How often is the router logs (covering administrator access /access control) reviewed?			A.10.10.1 A.10.10.2 A.10.10.5	
Are reports and analyses carried out based on the log messages?			A.13.2.2	
What is the course of action to be followed if any malicious incident is noticed?			A.13.2.1	
Security Updates				
Is the network engineer aware of the latest vulnerabilities that could affect the router?			A.6.1.7 A.12.6.1	The network engineer should receive periodic updates on the vulnerabilities and patches affecting the router.

source: http://www.TajDini.net

Mahyar TajDini (Mahyar@Tajdini.net)