

Audit Checklist #4 Major Risks Associated with Routers				
A. GENERAL CONTROL				
MAJOR RISK: FAILURE TO DRAW UP A PROPER POLICY FOR MANAGING, DEPLOYING AND CONFIGURING ROUTERS.				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
1. Has the organization drawn up a router security policy and has the router security policy been checked by those with expertise of the respective vendor's routers?				
2. Has the router security policy been approved, circulated, acknowledged, and accepted by those who deploy, service, configure and maintain the entity's router population?				
3. Does the policy take into account any individuals involved in any outsourcing contracts that the entity has placed for host or router maintenance?				
4. Does the policy make it clear who is authorized to access routers, and who is authorized to configure or maintain them?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
5. Does the policy make provision for variable levels of authorization and granting of different authorities for the purpose of router maintenance – where the operating system permits it?				
6. Has the organization’s policy made provision for the maintenance of appropriate logs/journals that show whom has access to routers and for what purpose?				
7. If response to step 6 is yes, are the logs/journals routinely or periodically reviewed?				
8. If response to step 6 is yes, are the logs retained for long enough to be useful for monitoring purposes?				

B. ROUTER DEPLOYMENTS				
MAJOR RISK: FAILURE TO DRAW UP PROPER PLANS FOR DEPLOYING ROUTERS.				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
9. Is there a formal planning process that defines, scales, deploys and integrates router services into the entity's network services?				
10. Does the organization take into consideration the vendor's advice about router management, configuration and security?				
11. Are there any internal or external Proof-of-Concept exercises benchmarking the existing architecture (including security features) and the results?				
12. Is there an agreed-upon process for deploying new or additional router services while minimizing disruption to other operational hosts or systems?				
13. Is there a process to ensure that all router personnel have proper training (vendor accredited) in management and security disciplines applicable to the organizations routers?				

C. BASE-LINING CONTROL				
MAJOR RISK: FAILURE TO DRAW UP PROPER BASE-LINING PROCEDURES FOR CONFIGURING ROUTERS.				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
14. Has the organization defined a security architecture in which the router services have a known and defined security role? If so, is this expressed by carefully structures and documented sets of router configuration rules which include access control lists/rules/filter settings?				
15. Has the organization appropriately defined router configuration builds for each security domain?				
16. Is there a complete and current archive of all router configuration builds which are properly commented for intelligibility? If so, are spare copies of these held in off-site secure storage?				
17. Is there a process that cross-checks (routine or ad-hoc) masters of router configuration builds against current configurations?				
18. Does the organization keep abreast of security vulnerabilities (notified by vendors and others)?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
19. Is there an agreed operating system (e.g. CISCO IOS) version and level of patching that forms the base-line software configuration?				
20. Is routine security and vulnerability scanning performed, and scanning whenever there is a major configuration change? Can different scanners be used simultaneously to ensure all vulnerabilities are covered?				

D. ROUTER SECURITY				
MAJOR RISK: FAILURE TO SET ROUTER HARDENING STANDARDS.				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
21. Has the facility removed all default router accounts, and removed all default passwords?				
22. Is there a minimum number of router accounts and do they have difficult-to-guess passwords?				
23. Does the facility distinguish temporary hires or contractors who might help to configure hosts within the system from permanent staff? If so, how do they accomplish this task?				
24. Has the facility configured master (secret), console, aux, and virtual terminal lines with difficult-to-guess and encrypted passwords? Are copies of these passwords or copies of configuration data secure from any unauthorized party?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
<p>25. Does the facility have an assurance that the absolute minimum number of TCP/IP Protocols, Services and Ports are permitted by the routing services?</p> <p>In particular, has the facility disabled:</p> <ul style="list-style-type: none"> a. Small services? b. SNMP? c. Remote Configuration, unless bounded by strong authentication? d. Ad-hoc or source routing (loose or tight)? e. HTTP? f. Finger? g. Broadcasts or Multicast Packets? h. ICMP redirects - generally, or alternatively, selectively filtering by ICMP type? i. All but the minimum number of ports necessary to provide a commercial service? 				
<p>26. Does the organization have an assurance that all other hosts deployed are using similarly hardened barebones software to which service packs, patches, corrections and fixes? Are they routinely applied?</p>				

E. PACKET ACCESS RULES				
MAJOR RISK: FAILURE TO SET PACKET BLOCKING STANDARDS.				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
27. Have all types of access control list been considered by the facility (e.g. CISCO standard, extended and reflexive)?				
28. Are old packet blocking rule lists erased prior to entering new packet blocking rule lists?				
29. Do blocking rules ensure that only internal addresses are permitted from internal connections to internal trusted networks, and only external addresses are permitted from external connections?				
30. Do blocking rules ensure that packets that are malformed or obviously fake blocked from external networks?				
31. Do blocking rules ensure that reserved network addresses and loopback addresses are blocked?				
32. Does the facility selectively filter ICMP redirects according to type?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
33. Is the facility blocking packets from untrusted networks (risks), undesired networks (content), or packets which carry the same source and destination address?				
34. Does the facility accept packets (telnet access to the router) from a limited number of trusted addresses and do they explicitly block all others?				
35. Where the facility has limited internetworking requirements in place, do they explicitly allow the required services from the required sources and explicitly deny all other accesses?				

F. ROUTE, ROUTE TABLE & HOST-TO-HOST CONTROLS				
MAJOR RISK: FAILURE TO SET UP ROUTE AND ROUTE TABLE CONTROLS.				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
36. Has the organization considered the security benefits/disadvantages of static versus dynamic routing tables?				
37. Have appropriate controls, authorization and integrity processes been put in place to ensure that routers cannot be spoofed with fake route updating information?				
38. Has the organization thought through and planned for migration to state-of-the-art security controls, including host-to-host and tunneling protocols?				

G. LOGGING CONTROLS				
MAJOR RISK: FAILURE TO PROPERLY SET UP LOGGING AND JOURNALIZATION CONTROLS.				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
39. Has the organization implemented router logging so that errors and blocked packets are recorded on a trusted host?				
40. Has the organization configured the logs so that port numbers are recorded?				
41. Is the logging host prevented from internal and external intrusions by appropriate access control, or from becoming the receiver of accidental or malicious log data?				
42. Would any individual within the organization be able to change router configurations and manipulate router logs without collusive activity?				
43. Has the organization properly considered the type and amount of log evidence that you will need to check and keep in order to provide an ability to investigate anomalies, attacks, system errors or to trace the source of system activity?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
44. Is there one particular individual or group within the organization that has been assigned the responsibility to examine logs and journals to ensure that activity was as intended?				
45. Are the logs set to include date/time information?				
46. Are the network and all hosts including routers and logging hosts running to the correct time? Is time maintained through an appropriate protocol such as NTP?				

H. COMMUNICATIONS AND SERVICE				
MAJOR RISK: FAILURE TO SET UP AN AVAILABILITY SERVICE LEVEL AGREEMENT.				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
47. Has the organization established a provision for the definition and measurement of availability and robustness of router based service?				
48. Is it understood as to who takes action when things go wrong and how issues will be escalated until they are resolved? If so, whom?				
49. Is one individual responsible for handling incidents concerning routers and take responsibility for intrusions into the organization's system? If so, whom?				
50. Has the organization adequately addressed issues concerning Business Continuity, Contingency Backup and Recovery, and Disaster Preparation connected with the router services that you are hosting?				
51. Has the organization's router support team clearly demonstrated their ability to meet service level, performance and bandwidth, and business continuity requirements?				

I. ROUTERS AND THE LAW				
MAJOR RISK: FAILURE TO PROPERLY EVALUATE FINANCIAL AND LEGAL MATTERS.				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
52. Does the organization have controlled processes to deal with router host software licenses?				
53. Is the organization responsible for the implementation of any legislative regulations concerning privacy or data protection?				