

**AUDIT PROGRAM
INTERNET FIREWALL REVIEW**

GENERAL BACKGROUND

The purpose of this program is to review and test the controls related to the implementation of firewall(s). The objectives in this area are to ensure:

1. Adequate security procedures are in place to manage the risks, threats and vulnerabilities resulting from network connectivity.
2. Controls over access from the internal network to the Internet and from the Internet to the internal network are functioning as designed.

OBTAIN AN UNDERSTANDING OF THE ENVIRONMENT

To prepare for the detailed audit procedures, obtain an understanding of the following areas relating to firewall configuration and management:

1. Internet policy of the organization.
2. Administration of the firewall.
3. Levels of available access to the Internet.
4. Configuration of the firewall.
5. Configuration of the internal networks.
6. Logging procedures for accesses to and through the firewall.
7. Control over access to the communication lines, firewall hardware and software.
8. Change control over the firewall configuration.
9. Firewall plan addressing business disruption or disaster.

**AUDIT PROGRAM
INTERNET FIREWALL REVIEW**

INDEX

<u>Areas of Review</u>	<u>Pages</u>
A. INTERNET POLICY	3-8
B. FIREWALL ADMINISTRATION	9-11
C. LOGICAL ACCESS CONTROLS	12-13
D. FIREWALL CONFIGURATION	14-17
E. INTERNAL NETWORKS CONFIGURATION	18-19
F. LOGGING PROCEDURES	20-22
G. PHYSICAL ACCESS CONTROLS	23-24
H. FIREWALL CONFIGURATION CHANGE CONTROL	25-26
I. FIREWALL PLAN	27-28

A. INTERNET POLICY				
CONTROL OBJECTIVE: The Internet policy should convey to all staff the intent of the controls to be implemented by the firewall.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Obtain a copy of the Internet Policy.				
2. Identify the process that was used to develop the policy. Ascertain whether the process considered the value of and degree of reliance on the firewall and the severity, probability, and extent of the potential for direct and indirect harm.				
3. Assess whether the policy: <ul style="list-style-type: none"> a. Identifies the specific assets that the firewall is intended to protect and the objectives of that protection (integrity, availability, and confidentiality). b. Describes the organizational structure and associated responsibilities and accountability of personnel who will be tasked with implementing the policy, monitoring compliance with the policy and adhering to the policy. c. Supports the use and flow of data and information. d. Documents what information passing through the firewall will be monitored. 				

A. INTERNET POLICY				
CONTROL OBJECTIVE: The Internet policy should convey to all staff the intent of the controls to be implemented by the firewall.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
4. Ascertain whether legal counsel has reviewed the policy to ensure consistency with requirements and limitations imposed externally (laws, regulations, etc.).				
5. Determine whether management approval of the policy has been sought and granted and the date of the most recent review of the policy by management.				
6. Identify how the Internet policy was communicated to users and how awareness is maintained. Select a sample of users and discuss their understanding of their responsibilities related to Internet use and how to report problems.				
7. Determine whether standards and procedures have been defined to specify the means by which the policy is implemented.				
8. Assess whether the standards and procedures specify who is responsible and empowered to do each function required for the proper operation of the firewall.				

A. INTERNET POLICY				
CONTROL OBJECTIVE: The Internet policy should convey to all staff the intent of the controls to be implemented by the firewall.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
9. Assess whether the security policy: <ul style="list-style-type: none"> a. Is easy to read and locate relevant sections. b. Is versioned and dated. c. Carefully worded with all ambiguous terms precisely defined. d. Sets out acceptable conditions of use as well as unacceptable conditions of use. e. Is widely communicated to affected persons. f. Is reviewed at regular intervals. 				
10. Consider whether the following issues are addressed in the policy document: <ul style="list-style-type: none"> a. Scope of the policy in relation to other internal and external networks with which it may be connected. b. Governing policies, such as law, contractual terms and conditions, or other policies internal to the organization. c. Frequency and necessity for reviews of the policy. d. Outline of the assets that must be protected, and from what threats. e. Security incident handling procedures. 				

A. INTERNET POLICY

CONTROL OBJECTIVE: The Internet policy should convey to all staff the intent of the controls to be implemented by the firewall.

AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
<p>11. Consider whether the rights and responsibilities of users are addressed in the policy document, including:</p> <ul style="list-style-type: none"> a. Account use, by both the account holder and the resource provider. Special conditions may apply to the use of normal user accounts and public access accounts. b. Software and data access and use, including sources of data and software. c. Disclosure of information which is potentially harmful, such as password information or configuration information. d. Etiquette, including acceptable forms of expression (e.g., non-offensive expression expected for unsolicited e-mail), and unacceptable practices (such as the forging of e-mail and news articles). e. Password use and format. f. Rights to privacy, and the circumstances under which the resource provider may intrude on the files held under or activities practiced by an account. g. Guidelines regarding reasonable practices such as the use of CPU cycles and temporary general access storage areas. 				

A. INTERNET POLICY

CONTROL OBJECTIVE: The Internet policy should convey to all staff the intent of the controls to be implemented by the firewall.

AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
12. Consider whether the rights and responsibilities of resource providers are addressed in the policy document, including: <ul style="list-style-type: none"> a. Physical security guidelines. b. Privacy guidelines. c. Security breach guidelines. d. Investigation of incidents guidelines e. Configuration guidelines, including: <ul style="list-style-type: none"> (1) Allocation of responsibility. (2) Network connection guidelines. (3) Authentication guidelines. (4) Authority to hold and grant account guidelines. (5) Auditing and monitoring guidelines. (6) Login banners. (7) Password format, enforcement and lifetime guidelines. 				

SUMMARY COMMENTS – PART A:

[Empty box for summary comments]

B. FIREWALL ADMINISTRATION				
CONTROL OBJECTIVE: Administration of the firewall should be restricted and should comply with the defined policy, standards and procedures.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Determine who is responsible for administering the firewall and their respective roles and responsibilities (e.g., configuration, backup, user administration). Assess whether segregation is effective in minimizing opportunities for security incidents, outages and personnel problems.				
2. Identify how the Internet policy was communicated to those responsible for administration. Discuss with them their understanding of their responsibilities related to the Internet.				
3. Assess whether access to administer the firewall is limited to a sufficiently small number of qualified staff. Ensure that the IP address is not the sole means of authenticating the administrator.				
4. Determine how the ability to administer the firewall is restricted. Obtain documentation identifying the staff with access to administer the firewall and check for compliance with information previously obtained.				

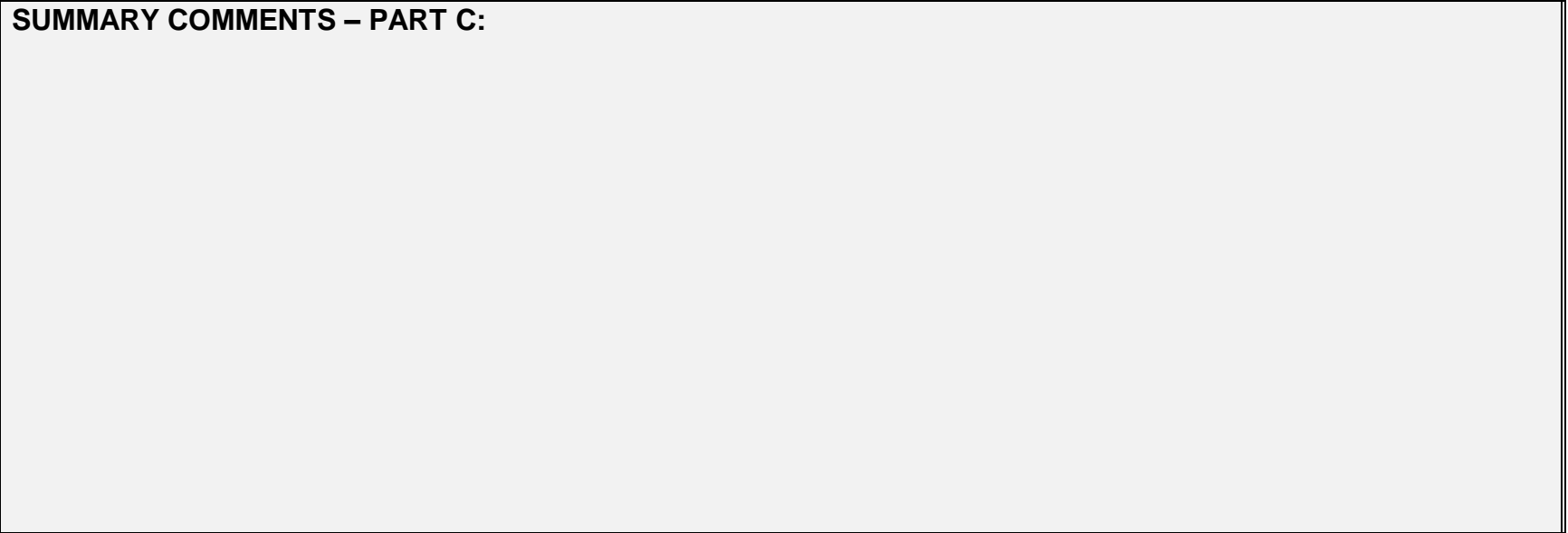
B. FIREWALL ADMINISTRATION				
CONTROL OBJECTIVE: Administration of the firewall should be restricted and should comply with the defined policy, standards and procedures.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
5. Determine whether the firewall can be administered while sessions are active.				
6. Determine what changes to the firewall, if any, impact on active sessions and what the impact will be (e.g., denial of ftp while an ftp session is active).				
7. Identify the frequency with which firewall components are backed up and where the backups are stored.				
8. Determine who is responsible for keeping up with current security advisories and how this responsibility is carried out.				
9. Determine whether the security administrator reviews changes to the network to ensure security is not compromised.				

SUMMARY COMMENTS – PART B:

A large, empty rectangular box with a thin black border, intended for entering summary comments. The interior of the box is light gray.

C. LOGICAL ACCESS CONTROLS				
CONTROL OBJECTIVE: Access to the Internet should be authorized.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Identify how employees and non-employees are authorized to have Internet access and the levels of access available. Identify how access to the Internet is changed or revoked. Assess the timeliness and completeness of the methods used.				
2. Print a list of the users with access to the firewall and cross-check this lists against the current employee list and access authorizations. Follow-up on any discrepancies.				
3. Determine whether employees are given special privileges to enable firewall administration. Review the access granted and ensure that it is no more than the access needed.				
4. Determine whether the security administrator periodically reviews the list of who has access to the firewall. Identify the date of the most recent review and cross-check against supporting documentation.				

SUMMARY COMMENTS – PART C:

A large, empty rectangular box with a thin black border, intended for entering summary comments. The interior of the box is light gray.

D. FIREWALL CONFIGURATION				
CONTROL OBJECTIVE: The firewall should be configured to enforce the security policy (including encryption, viruses, URL block and packet filtering)..				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Identify the rules that should be enforced by the firewall (what services are allowed between what source and destination and when).				
2. Obtain the Security Manual for the firewall.				
3. Identify what services (if any) are encrypted and the encryption scheme used.				
4. Determine whether URL screening is being performed by the firewall. If so, determine how the list of URL's is administered and maintained.				
5. Determine whether anti-virus inspection is enabled. If so, identify what 3 rd party application is used for anti-virus screening.				
6. Determine whether packets are screened for the presence of prohibited words. If so, determine how the list of words is administered and maintained.				
7. Determine whether intrusion detection is automated.				

D. FIREWALL CONFIGURATION				
CONTROL OBJECTIVE: The firewall should be configured to enforce the security policy (including encryption, viruses, URL block and packet filtering)..				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
8. Identify the threats for which response has been automated (e.g., denial of service attacks, spoofing).				
9. Identify whether the firewall files are cryptographically checksummed and those checksums are regularly verified.				
10. Determine whether the effectiveness of the firewall is periodically tested from both sides.				
11. Review the processes operating on the firewall at the time of the audit and assess whether they are appropriate and operating properly.				
12. Determine what authentication strategy is used and how it is administered.				
13. Determine whether the firewall provides adequate notice to anyone (internal or external) attempting to exploit them.				

D. FIREWALL CONFIGURATION				
CONTROL OBJECTIVE: The firewall should be configured to enforce the security policy (including encryption, viruses, URL block and packet filtering)..				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
14. Identify the standard protocols and any non-standard protocols used.				
15. Determine whether the firewall uses dynamic or static address translation.				
16. Determine what controls are in place to prevent denial of service attacks.				
17. Determine whether incoming Java or ActiveX code is permitted. If so, identify what screening has been implemented.				
18. Determine whether there are controls in place to detect spoofing.				
19. Assess whether the firewall implementation effectively enforces the approved security policy.				

SUMMARY COMMENTS – PART D:

[Empty box for summary comments]

E. INTERNAL NETWORKS CONFIGURATION				
CONTROL OBJECTIVE: The internal networks should be configured to prevent inappropriate access from the Internet and enable prompt detection.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Obtain a technical diagram that shows the network and the firewall, with IP addresses.				
2. Assess whether the firewall properly separates the DMZ (demilitarized zone) from the inside network and the outside network.				
3. Determine whether there is a single point at which the internal network can be separated from the Internet.				
4. Identify the monitoring and control procedures used on the internal network to enforce security. Review supporting documentation to ensure the procedures are being followed.				

SUMMARY COMMENTS – PART E:

[Empty box for summary comments]

F. LOGGING PROCEDURES				
CONTROL OBJECTIVE: Accesses to and through the firewall should be logged and procedures should be in place to monitor and act upon any inappropriate activities.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Determine what firewall activities and events are logged. Ensure that inbound services, outbound services, and access attempts to or through the firewall that violate the policy are all logged.				
2. Identify the monitoring procedures used on the firewall to detect security breaches and attacks. Differentiate between automated and manual procedures. Identify how frequently the monitoring is performed.				
3. Determine whether alarms have been set for significant events or activities.				
4. Assess whether the person responsible for responding to alarms or monitoring the firewall is experienced in information security and the operation of the firewall.				
5. Get a copy of any reports provided by the firewall.				
6. Assess the ease with which the information recorded and reported by the firewall allows attacks, defenses, configurations and user behavior to be analyzed.				

F. LOGGING PROCEDURES

CONTROL OBJECTIVE: Accesses to and through the firewall should be logged and procedures should be in place to monitor and act upon any inappropriate activities.

AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
7. Identify the process used to follow-up on and resolve any incidents and the documentation prepared to support the process.				
8. Determine whether the actions of staff who have privileged access to the firewall are authenticated and monitored.				
9. Determine whether the effectiveness of the firewall in enforcing the Internet policy is reported to management.				

SUMMARY COMMENTS – PART F:

[Empty box for summary comments]

G. PHYSICAL ACCESS CONTROLS				
CONTROL OBJECTIVE: The communication line, firewall hardware and software should be secured to prevent unauthorized access.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Determine the specifications of the communications line used to access the Internet.				
2. Assess the vulnerability of the communications line to unauthorized physical access.				
3. Determine how, and to whom, phone numbers and circuit IDs are disseminated.				
4. Identify how updates of the firewall software are secured and distributed.				
5. Identify the physical controls over the firewall and ensure that they are comparable to the controls over the information and assets the firewall is expected to protect.				
6. Ensure that all firewall components, including those devices used to manage the firewall, are within the same secure perimeter.				

SUMMARY COMMENTS – PART G:

Empty rectangular box for summary comments.

H. FIREWALL CONFIGURATION CHANGE CONTROL				
CONTROL OBJECTIVE: Changes to the firewall configuration should be authorized and tested prior to implementation.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Obtain a copy of the documented procedures for requesting, authorizing, implementing and testing changes to the firewall.				
2. Assess whether remote administration is possible and the controls in place to support it (one-time passwords, other secure authentication or encrypted link).				
3. Identify whether changes to the configuration can and are tested in a safe environment. Determine whether there is a method for easily and quickly backing out changes.				
4. Determine whether there is an independent method of comparing two configurations to identify differences and verifying those differences against change control information. Identify the frequency with which such comparisons are carried out.				
5. Determine whether configuration management is automated and simple to prevent errors from occurring.				

H. FIREWALL CONFIGURATION CHANGE CONTROL

CONTROL OBJECTIVE: Changes to the firewall configuration should be authorized and tested prior to implementation.

AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
6. Ascertain whether the firewall security is reassessed whenever the firewall is significantly changed.				

SUMMARY COMMENTS – PART H:

Large empty rectangular area for summary comments.

I. FIREWALL PLAN				
CONTROL OBJECTIVE: A firewall plan should be developed and tested to ensure recoverability in the event of a business disruption or disaster.				
AUDIT PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Determine whether a firewall plan has been developed based on an assessment of the continuity requirements.				
2. Assess whether acceptable time limits have been specified for reset and recovery.				
3. Ascertain whether the plan is regularly tested.				
4. Review the results of the most recent test and determine whether the plan was updated accordingly.				

SUMMARY COMMENTS – PART I:

[Empty box for summary comments]