Security regulations and audits go beyond firewall policies and implementation, but it’s a good place to start for audit-readiness and getting a continuous visibility of your network.

The following steps can ensure that you are ready for your next firewall audit.

1. **Gather Important Information**

For your firewall audit to be successful, it’s important that you understand what is in your network. Make sure to collect all firewall logs and security policies that are relevant for you to analyse. Develop a diagram of your network and firewall topologies. Collect all previous audit documentation, including objects, firewall rules and policy revisions. Also review your vendor information such as the version of your OS, default configuration and latest patches.

Once you gather the information, it’s important to integrate and arrange this information in easily legible and illustrative manner.

1. **Review Firewall Change Management Process**

Two common issues of firewall change management are poor documentation of changes and validation of their impact on the network. Employee turnover and poor records of why the change was made make it difficult to make a decision on what you need to do. Always review your procedures for rule-based maintenance to determine whether you have:

* A controlled and formal process for requesting, reviewing, approving and implementing firewall changes
* All changes that are authorized or not, and flag unauthorized changes for further review.
* Enabled real-time monitoring of firewall changes with rule-changing access granted to authorized personnel or not.

1. **Conduct a Physical and OS Security Audit of your Firewall**

Ensure that your management servers and firewalls are physically secure and have controlled access to them. Also review that your operating system should pass hardening best practice checklist. By enforcing these baselines and reporting against them, you can be knowledgeable about your firewall’s configuration status.

1. **Clean Up and Optimize the Rules**

Remove unnecessary overheads in your firewall audit by cleaning up on rules that no longer apply. Identify unused objects and rules along with covered rules, consolidate all those that are similar and make overly permissive rules stricter.

1. **Conduct Risk Assessment and Remediate the Issues**

When you review your firewall rules and configuration, try to identify those that are potentially risky. The term “risky” is relative to every organization, depending upon the network and acceptable risk level. However, you can use many standards and frameworks to get a reference point. Prioritize your risky rules by their severity. Once done, document and create an action plan to remediate risks and compliance exceptions.

1. **Ensure Readiness for Ongoing Audit**

For firewall configuration, you need to maintain a firewall audit readiness as a business process. Automate your process and get more done in lesser time. Moreover, creating a solid change management process and proper documentation can ensure that you are ready for an audit.

Get in touch with Aardwolf Security today to start your Firewall audit-readiness journey.