A build review evaluates the configuration of a device, operating system and its settings against certain industry standards. It plays an important role in creating a strong security posture for an organization. It provides consistent and established testing that helps security and IT teams in understanding whether and how effective their configurations are in protecting the infrastructure against cyber attacks.

A build review is also vital in early identification of issues during the deployment process. Hence, it helps avoid an issue from becoming a recurring problem down the road.

## What does a Build Review Include?

Build reviews generally include the following in their scope:

* User privileges and permissions
* Operating systems versions and patch checking
* Reviews of third-party software
* Service permissions
* Security policy configurations
* Event logging and auditing
* Password and locking policy
* Share and access permission
* Connectivity or network configuration reviews
* Anti-virus and firewalls review
* Physical review including encryption, boot options, media ports and BIOS protection
* Desktops, laptops, kiosks, servers, mobile and networking devices
* Virtual, physical and docker images
* Company policies audit reviews

## What is Involved in a Server Build Review?

A server is a backbone of a business infrastructure. Thus, it’s important to have a deeper security posture analysis of a server. Server build review involves the following important measures:

* A comprehensive analysis of each aspect of server security
* Analysis of server applications implemented on an operating system
* Benchmarking of infrastructure against the government and industry security standards
* Providing detailed report on any non-conformance, along with a priority list of remedial actions

## Why is a Build Review Important?

A build review helps us understand vulnerabilities in software and hardware configurations so that we can remediate them before they become a long-term problem or turn into an actual cyber threat.

As an initial cyber security review, it helps us identify our present cyber security risk posture. Hence, it allows us to define a baseline strategy to make continuous and ongoing improvements for the future.

Briefly, a build review has the following benefits:

* Provides knowledge about vulnerabilities
* Shortens potential downtime
* Reduces the chances of making mistakes in future deployments
* Exposes potential cyber threats
* Ensures correct configurations
* Ensures an improved security posture.

## Why Choose Aardwolf Security’s Build Review Services?

Our build reviews cover all major Operating Systems. We identify key gaps and provide a detailed report based on those gaps. Moreover, our team consists of expert consultants who are well versed in auditing of server systems.

Contact us today to find out more about how we can help you.