IBHAMU LIMITED

PROFESSIONAL SERVICES · WHITEPAPER

Infrastructure Audit Checklist

The framework our engineers use to assess an environment before recommending any changes.

HOW TO USE THIS CHECKLIST

A structured way to assess what you’re actually running.

Most infrastructure decisions get made against what the documentation says is running, not what’s actually running. This checklist is the starting framework our engineers use to close that gap before recommending any changes — covering servers, network, security posture, backup integrity, facility conditions, and documentation gaps in one pass.

It’s built to be used two ways: by an internal IT team running a self-assessment ahead of a budget cycle, or as a way to sanity-check a vendor’s proposed audit scope before you commission it. Work through each section in order — later sections often surface issues that explain findings from earlier ones.

SECTION 01

Server & Storage Inventory

Start with what’s physically and virtually deployed — most audits find at least one server nobody remembered was still running.

- [ ] **Document every physical and virtual server**
  Make, model, age, and current role for each one.
- [ ] **Record OS versions and patch levels**
  For every server, not just the ones considered critical.
- [ ] **Identify hardware past vendor end-of-life or end-of-support**
  These carry disproportionate risk even if currently stable.
- [ ] **Map storage capacity, utilization, and 12-month growth trend**
  Sizing decisions should follow data, not guesswork.
- [ ] **Confirm RAID / storage redundancy configuration**
  Verify on every array, not just the ones you remember configuring.
- [ ] **Identify single points of failure in the server estate**
  A single switch, server, or power feed that would take down multiple systems.
- [ ] **Verify server room and rack labeling matches documentation**
  Mislabeled equipment costs time during an actual incident.

SECTION 02

Network Topology Review

Undocumented network growth is the norm, not the exception — this section produces the as-built picture most environments are missing.

- [ ] **Produce or validate an as-built network diagram**
  Compare it directly against what's physically connected.
- [ ] **Identify redundant vs. single-path links between critical sites**
  A single fiber cut shouldn't isolate a location.
- [ ] **Review VLAN segmentation against intended access policy**
  Confirm traffic is actually isolated the way it's meant to be.
- [ ] **Test failover on redundant WAN or ISP connections**
  Confirm it actually works, not just that it's configured.
- [ ] **Confirm firmware versions on core switches and routers**
  Check against current vendor security advisories.
- [ ] **Identify unmanaged or undocumented network devices**
  Rogue access points and unmanaged switches are common findings.
- [ ] **Review wireless coverage against actual usage areas**
  Not just where access points happen to be mounted.

SECTION 03

Security Posture Baseline

This section is a baseline, not a penetration test — it tells you where a deeper security assessment is most urgently needed.

- ☐ **Review firewall rule sets for unused or overly permissive rules**
  Rules accumulate and are rarely cleaned up.
- ☐ **Confirm multi-factor authentication on administrative access**
  This is the single highest-leverage control in most environments.
- ☐ **Review the most recent penetration test or vulnerability scan**
  If neither exists, that’s itself a finding.
- ☐ **Confirm endpoint protection is installed and current**
  Across all devices, including ones IT doesn’t directly manage.
- ☐ **Review the privileged account list**
  Remove access for anyone who no longer needs it.
- ☐ **Confirm logging is centralized with adequate retention**
  You can’t investigate an incident you didn’t log.
- ☐ **Review VPN / remote access configuration and user list**
  Including access still active for former staff or contractors.

SECTION 04

Backup & Recovery Verification

A backup that has never been restored is a hypothesis, not a safeguard — this section tests the assumption directly.

- [ ] **Confirm backup jobs are completing successfully**
  Not just that they're scheduled to run.
- [ ] **Test a full restore from backup**
  Not just a single file-level restore.
- [ ] **Confirm retention meets your regulatory or business requirements**
  Retention periods are often set once and never revisited.
- [ ] **Verify backups are stored offsite or in a separate failure domain**
  A backup in the same room as the server protects against nothing.
- [ ] **Document the actual recovery time achieved during testing**
  Compare it against your required recovery time objective.
- [ ] **Confirm backup encryption for data at rest and in transit**
  Especially for backups leaving the primary site.

SECTION 05

Facility & Environmental Conditions

Facility failures — power, cooling, fire suppression — take down otherwise healthy infrastructure. This section is often skipped by IT-only audits.

- ☐ **Confirm UPS battery health and last load-test date**
  A UPS that hasn’t been load-tested is an assumption, not a safeguard.
- ☐ **Review generator maintenance and fuel reserve, if applicable**
  Confirm the last test run and its actual duration.
- ☐ **Confirm cooling capacity against actual heat load**
  Sized against equipment output, not just floor area.
- ☐ **Inspect for dust, cable strain, or containment gaps**
  Small physical issues predict bigger failures.
- ☐ **Confirm fire suppression was tested in the last 12 months**
  Clean-agent systems specifically, for an electronics environment.
- ☐ **Review physical access control logs**
  For the server room or data centre specifically.

SECTION 06

Documentation Gap Analysis

The most common single point of failure in any environment is a person, not a server — this section maps where that risk sits.

- [ ] **Identify systems with no current documentation**
  Start with whatever came up most during this audit.
- [ ] **Identify institutional knowledge held by only one person**
  What happens if that person is unavailable during an incident?
- [ ] **Confirm diagrams reflect current state, not a past state**
  A diagram that’s wrong is often worse than no diagram.
- [ ] **Review vendor support contracts and renewal dates**
  Lapsed support contracts are a common, avoidable risk.
- [ ] **Confirm an incident response plan exists and was reviewed this year**
  A plan nobody has read recently isn’t a plan.

NEXT STEPS

What to do with the findings.

A completed checklist usually surfaces more findings than one team can reasonably act on at once. The next step is prioritization — typically starting with anything touching business continuity (backup integrity, facility redundancy, single points of failure) before moving to optimization work.

If you'd rather have this run independently — or want a second opinion on findings from an audit you've already completed — that's exactly what our Professional Services practice does.

ibhamulimited.com/contact.php

info@ibhamulimited.com · +234 700 000 0000