Network and System Audit

Logic Finder takes pride in providing Network and System Audit of medium to large enterprises. We use variety of tools and use a well-defined methodology to assess infrastructure. We can also provide network security audit if required by the customer

Table of Contents

Network and System Audit 1

1. Executive Summary: 3
2. Introduction: 4
3. Project Scope: 5
4. Audit Methodology: 5
5. Terms and Abbreviations 6
6. Network Auditing Initial Phases: 6
7. Network Auditing Process: 7
8. References 8

1. Executive Summary:

Network auditing is the collective measures done to analyze, study and gather data about a network with the purpose of ascertaining its health in accordance with the network/organization requirements. Network auditing primarily provides insight into how effective network control and practices are, i.e. its compliance to internal and external network policies and regulations.

LogicFinder can identify problems and provide the corrective actions, while working alongside with a company to map their network infrastructure and identify weaknesses and vulnerabilities. Our aim is to make any problems easy to understand and fix them as quickly as possible. Our experienced team can pinpoint security holes that leave your network vulnerable to hackers, poor-practices, and actions from internal employees.

Companies that lack the network experience or knowledge get in danger of future costs associated with repair or replacement network solutions. LogicFinder can provide essential services to confirm that network are working in right way and can create optimized solutions. The analysis of the evidence obtained during the audit determines if there are gaps in the information systems and a technology management strategy and plan is developed to ensure that the IT assets are operating effectively.

LogicFinder does network systems audit by:

- Reviewing the design, configuration and implementation of the network systems
- Checking that the businesses computing facilities operate in a controlled and efficient manner
- Assessing whether data held on computing and communication facilities is stored in a secure and controlled manner
- Reviewing IT system security including location of computing and communication facilities, data storage and backups
- If applicable, auditing compliance by staff with the site's IT policies, such as file access permissions, group and password policies.
- Preparing a detailed asset listings for all servers and desktop computers
- Reviewing the printer network configuration to ensure their productive utilization
- Present findings and a Technology Management Strategy and Plan with recommendations
- Assists to enact the Plan and ensure its actions are completed

2. Introduction:

Given the complex IT and fast changing business environment in a highly connected world, IT network audit has increasingly become a critical component of an effective network performance and IT operations. The purpose of this project is to perform a thorough IT audit and network assessment to optimize the network infrastructure, discovering capacity issues, security faults, improve network capacity to reduce costs and deliver real business value. An in-depth review is conducted and report of all network hardware and software issues is delivered.

Nowadays, IT departments are facing big challenges such as under constant pressure to prove their return on technology investment. IT leaders face further challenges such as; compliance, security, big data, IoT, digital transformation which makes IT auditing an essential priority.

Network auditing is a process in which the network of an organization is mapped both in terms of software and hardware. The process can be daunting if done manually, but luckily some tools can help automate a large part of the process. The administrator needs to know what machines and devices are connected to the network. The information of what operating systems are running and to what service pack/patch level is also required. Another point on the checklist is what user accounts and groups are on each machine as well as what shares are available and to whom. A good network audit will also include what hardware makes up each machine, what policies affect that machine and whether it is a physical or a virtual machine. The more detailed the specification; the better it is.

Once the machines running in the network that are mapped, the administrator then moves to audit what software is running on each of the machines. This can be done manually, through an application, or simply asking each machine owner to run a script that would automatically catalogue applications and send the administrator an email with a report of the software installed. After the software inventory is done, the process can then catalogue the services which are installed, which are running and which are stopped. The audit for the machines can be finalized by noting which ports each machine listens on and what software is running at the time of the audit.

Once the administrator completes auditing the computers on the network, the next step is moving on to cataloguing the devices. These can include printers, fax machines, routers, access points, network storage and any other device that has connectivity with the network. Once this is done, the network audit would be complete and then the data collected is analyzed. The questions related to each specific network are addressed and machines that were not up to standard are brought inline, and an effective inventory baseline for all machines on the network becomes available.

3. Project Scope:

The main objective of this project is to:

- Identify and establish a set of expected standards for the management and security of every network connected to the backbone
- Examine the extent to which every network meets these standards
- Provide an overall review of the consistency, quality, and reliability of the network management processes
- Identify opportunities for improvement.

4. Audit Methodology:

LogicFinder provides a comprehensive Audit and Compliance service that touches every vertical of network and operations of an organization. This service not only aims to identify gaps and non-adherences, but also recommends improvement plan and strategy, implementation roadmap, cost-benefit analysis, quick wins, certifications etc. LogicFinder engages a specialized team of technology and process experts who follow a consultative approach to meet specific business and operational needs of a customer. Moreover, we extend our support for recommendation and implementation as a partner enabling the customer to cease maximum benefits.

The typical audit approach is depicted below:

Network Audit Strategy:

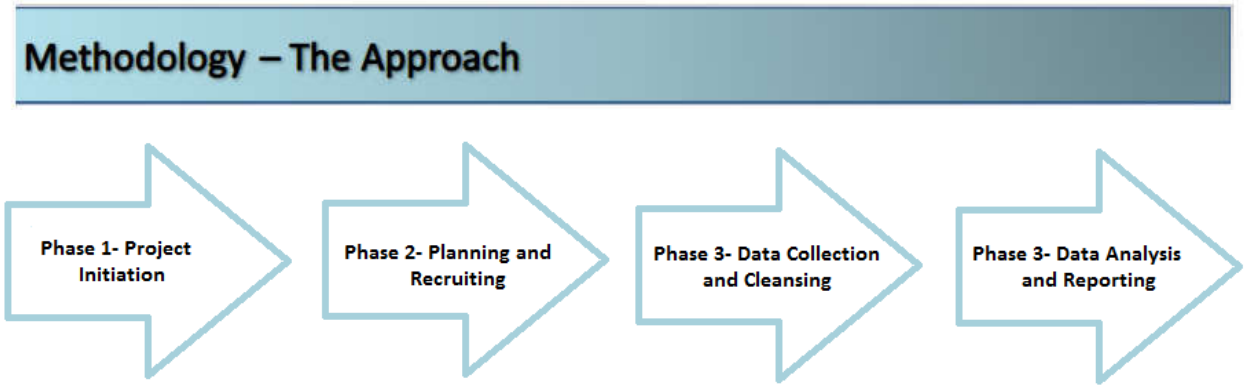


Figure 1: Network Auditing Phases

- Assessment and independent view of an organization's network strategy, scalability and approach
- Analysis of network architecture
- Validation of network expansion strategies
- Analysis of rolled-out network specifications
- Assessment for implementation of new technology with the current available network design

Logical Network Audit:

- Assessment of network resiliency plans

- Assessment of standard configuration against existing configurations
- Identifying bottlenecks and unwanted configurations for clean-up
- Capacity assessment leading to optimization of the network
- Circuit record reconciliation and verifications

Performance Audit:

- Assessment to check obsolescence of operations (process / technology / practices)
- Assessment of bottle necks that impact productivity
- Assessment for optimization of operations to enhance productivity
- Dashboard Assessment (based on defined network KPI)

Site & Infrastructure Audit:

- Assessment of passive network infrastructure like fiber, shelter, tower and related components.
- Physical Site Surveys
- Assessment of planned versus implemented physical site parameters on field
- Assessment of active physical equipment's (routers, switches, ports, etc.)
- Assessment of space, power, aircon and related site infrastructure.

Network Security Audit:

- Assessment of technology vulnerabilities
- Network and data security, privacy and compliance audit
- Device management and security
- Application management and security
- Penetration testing
- Intrusion detection and prevention

5. Terms and Abbreviations

MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
Switch	A device that receives incoming data packets and redirects them to their destination on a local area network
Router	A networking device that forwards data packets between computer networks
Firewall	A network security device that monitors incoming and outgoing network traffic
SNMP	Simple Network Management Protocol
SSH	Secure Shell, cryptographic network protocol

6. Network Auditing Initial Phases:

At the initial meeting with client requiring network audit, the LogicFinder will:

- Provide an outline of the scope of the audit project: What network functions will be included.
  - Administration
  - Security
- Discuss the security of servers and workstations considering: physical & logical security, environmental controls, and the operating system controls necessary to ensure the integrity of the server and clients.

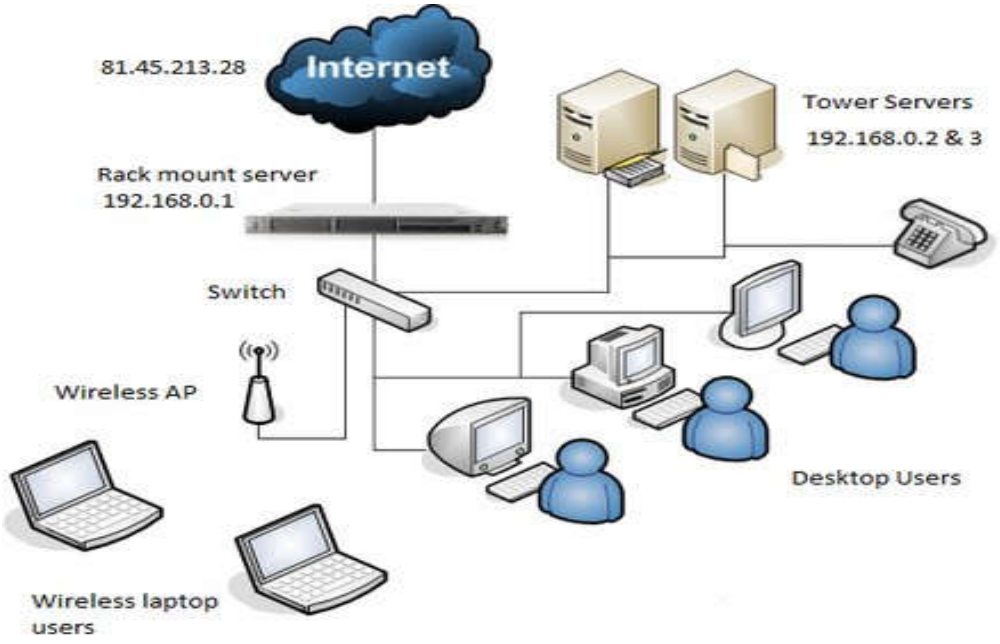
- Number of servers and operating systems
- Number of users per workstation and operating system
- Is there a LAN/PC policy?
- How access to the system, the server and the resources on the server (printers, files, directories, etc.) are controlled:
  - use of intruder detection, console and operators;
  - policy on passwords, access rights assignment, inactive accounts;
  - What data and applications are run on the network? Measures to guard against risks of confidentiality, unauthorized use, and access from both internal and external users.
- Discuss what virus protection measures are in place.
- Discuss LAN utilization and activity reporting: whether logs of system, downtime, accounting and audit (e.g., AUDITCON) have been activated and used; whether irregular activities and sniffing can be prevented and detected.
- Discuss backup and recovery procedures and whether data stored on the system can be restored in an orderly manner from the backup media.

7. Network Auditing Process:

For performing network audit for an organization there are too many things that need to be monitored and analyzed. Following parameters need to be checked:

- Checking the switches, routers, and load balancers.
- Checking cabling infrastructure.
- Checking the MPLS network and its configuration.
- Checking Servers, firewalls, configurations etc.
- Checking software, application and antivirus.

And on the basis of the outcome a cost effective and best solution is presented to organization.



8. References

1. https://www.citizensfla.com/documents/20702/2847745/20160927+02H+OIA+2016-AUD-IT-01+Network+Design+and+Architecture+Report+Executive+Summary+.pdf/e89c9822-434e-4e52-88f1-170a7aa9a332
2. https://www.routerfreak.com/how-to-perform-network-audit/
3. https://www.mcgill.ca/internalaudit/audit-objectives-and-processes/primary-project-types/computer-network-audits