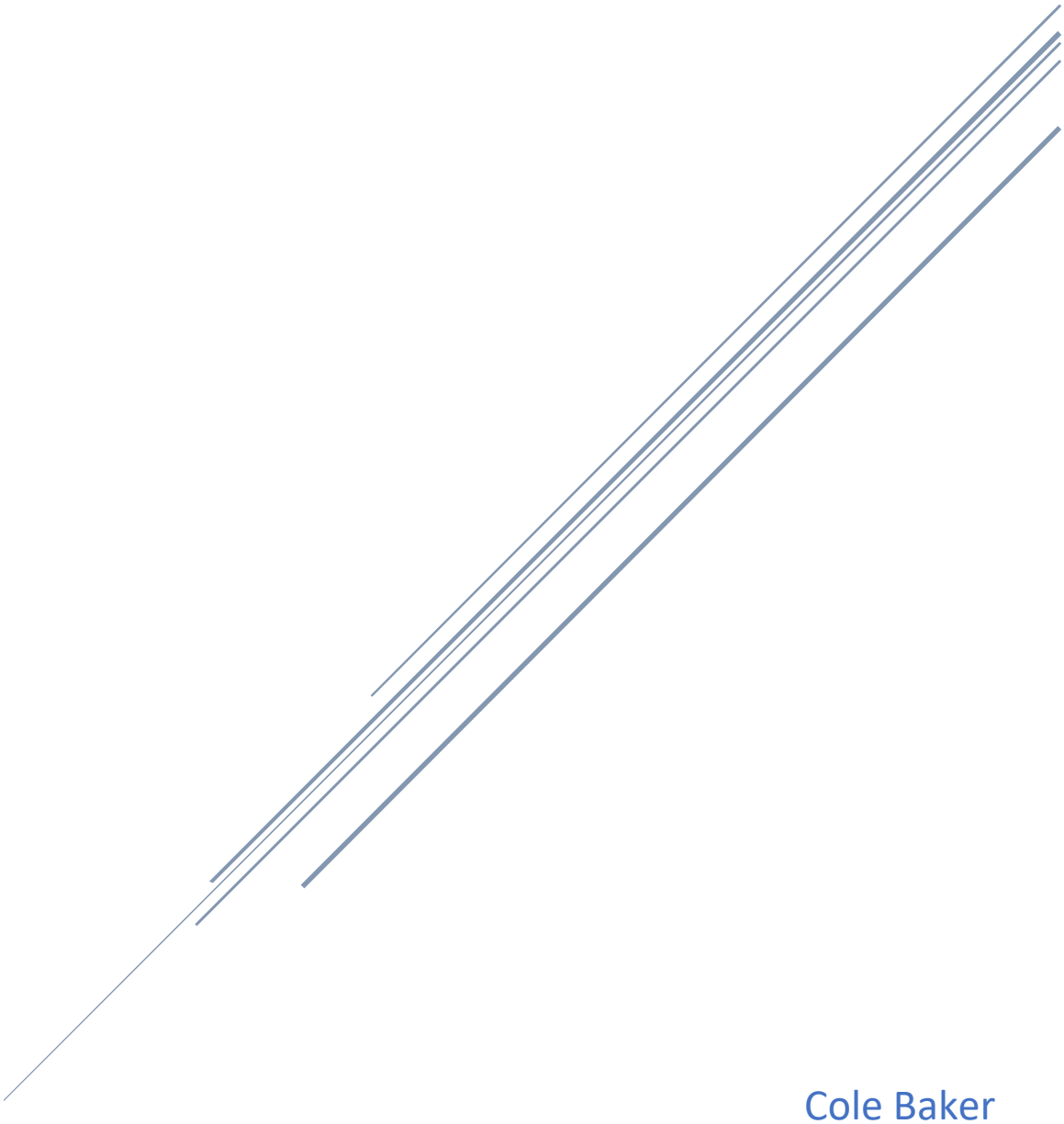
AUDIT REPORT - EXAMPLE



Cole Baker

Table of Contents

Task 1 – Audit Report 2
Statement of Audit Scope 2
Executive Summary 2
Issues and Solutions 2
Task 2 – Example Audit Report 3
Overview of Audit Report 3
Executive Summary 3
Scope of Audit 4
Control Procedures 4
Audit Results - Important 4
Auditing Plan 6
Control Procedures 7
References 8

Task 1 – Audit Report

Statement of Audit Scope

The scope of a report must provide an outline and results for auditing tests performed on the defined system. The scope must include any policies that will be reviewed, including any policies that my not directly effect the system but may have access to the system at any time. Such as for a router, a BOYD policy should be reviewed to ensure that system that relates to the primary audit focus is being audited correctly. In addition to audit policies, all audit settings and configurations must be reviewed to ensure that the auditing system is functioning correctly and that no configurations have been modified.

Executive Summary

The executive summary must include any information about the upcoming or performed audit that may need to be presented to the primary authority for the device such as the CEO or the IT department head. This section should include any matter that may require the executive's insight on such as financial matters or critical issues that are found during the audit. It should also include any information found within the scope. The summary must include what will be audited, how issues and solutions will be recorded. This should also include information about the business, such as size of the business or how many employees that may need to be defined later. Basically, anything important to this report should be in here or the CEO won't be happy.

Issues and Solutions

This section of the report can be presented in many different formats, but they all do the same thing, they show any results found from the audit. Any issues will have to be laid out along with their solutions, in some cases, these may need to be presented in the executive summary if the issue is rated as a critical or something along those lines. The issues and solutions section of an audit report is normally the most important of an audit report. This section could delay an upcoming update to the infostructure if the audit grades a fail to the company. This section could also present to the management staff any financial requirements that may come into play if some features or issues require new equipment or expensive upgrades.

Task 2 – Example Audit Report

Overview of Audit Report

This audit report will provide detailed results from an audit conducted on a network connected by a series of router.

Executive Summary

The following section contains an overview of all information covered by this report. This section is intended for review by the appropriate authority, such as a CEO, Project Manager or IT Department head. This section should help this authority better understand every detail of the following audit.

During this audit, conducted by the primary auditor Cole Baker, the following information and features were assessed. The auditor has compiled an "Audit Results" section at the end of this report to review and highlight the information obtained from this audit.

The following features, parameters and polices have been included in the audit and their results are contained below. This section will also provide a snippet of the results for any feature, parameter or policy that received a fail or presented an issue.

- Logging Policy
- Password Policy
- BYOD Policy
- Connection Setting
- Configuration
- System Performance
- Installed Features
- Security Protocols
- Any policy or feature that may not be directly connected to the network router but may have an effect on the operation of the device.

The following sub-section of the executive summary will give the reader a snippet of any issues found during the auditing process of this report. Full detail for these results can be found in the "Audit Results" section as well as any solutions the auditor has recommended for remediation.

<u>Issues Snippet</u>

- Insufficient BYOD Policy: During the audit of the network router, the auditor found that the BYOD Policy was insufficient for securing devices that may come in contact with the network router.
- Logging Policy Failure: During the audit of the network router, the auditor found that the logging policy and configuration was unsuccessful at logging multiple types of data, such as changes to the system configuration, or access to the device.

Scope of Audit

This report will detail what will be and what will not be audited by the primary auditor Cole Baker. The auditor will work with technical staff to ensure that there is a complete understanding of how the network router operates to ensure that there are no false issues presented during the audit. The auditor will only be auditing the primary network router and any policies, features or parameters that may have an effect on this device. No other devices in the organization should show up in the process of this audit. If changes must be made to this report, it must than be re-approved for proceeding. The auditor will be auditing all security implementations to this device as a focus to ensure data and sensitive information is secure. The auditor will focus on security to ensure that security is present at every level. After this audit is complete the auditor hopes to provide insight in the possibility of extending the organizations infostructure, as well as to reduce any security risks that are present.

Control Procedures

This following section will provide insight into the procedures that must be take in the event of a delay in the audit or if any critical security issues are found during the audit as well as how they will be recorded in the "Audit Results" section of this report.

In the event of a delay in the auditing process due to weather/power issues preventing the auditor from accessing the device, or other internal delays. The auditor will avoid auditing the BYOD Policy and the Installed Features audit, to ensure that all of the critical aspects are audited.

In the event of the auditor finding any critical issues that would present a major security risk to the device or the organization. The audit will present this information to the appropriate authority immediately and record this incident in the "Audit Results" section in the following format.

- **Critical** – Date/Time – Title of Issue – Feature, parameter or policy
  Description of Issue

Audit Results - Important

The following section will detail and display all results found during this audit report. As seen in the section title, this section has been marked as Important, this section is the final results of the audit report compiled by the primary auditor. The following results will be listed as a pass or fail grade, in the event that a result is given a fail, the entry in the results will include the solution to the issue presented. Any result marked as a fail will be listed first as these issues will need to be attended to as soon as possible.

Feature, Parameter or Policy	Results	Solution (if applicable)	Pass or Fail
Logging Policy	During this audit, the auditor found that the logging policy was not logging multiple data types. The logging configuration was not correct.	Re-configure the logging system and ensure that the system is logging correctly by using testing. Attempt to log in with an incorrect password and ensure the logging system captures that attempt.	Fail
Connection Setting	The auditor found that all connection settings and any connection methods are functioning as intended.	Not Applicable	Pass
Installed Features	The auditor found that all installed features were up to date and in use	Not Applicable If any features become unused, disable or delete them	Pass
Password Policy	The auditor found that there was strong password policy in place that was being enforced by management staff. The Policy forced a user to create a password with at least 8 characters, special symbols.	Not Applicable	Pass
System Performance	The auditor found that the network router was running at optimal condition and the bandwidth was at full speed.	Not Applicable	Pass
BYOD Policy	The auditor found that the BYOD Policy that is currently in place does	The BYOD policy must be re-written to include how the device	Fail

	not provide sufficient parameters to keep the network router secure from any threats that the BYOD device may present to the environment.	must be setup, such as should include a mobile anti-virus as well as the latest OS and app updates. It should also include what the device is allowed to connect to.	
Configuration Settings	The auditor found that the configuration of the network router was setup correctly as specified by the action plan that was reviewed.	Not Applicable	Pass
Security Protocols	The auditor found that the network router has a greater than sufficient amount of security features in place, such as firewalls in place, IDS systems and Endpoint monitoring.	Not Applicable	Pass

Auditing Plan

"This section should be included in most or all audit reports. This section would lay out how the auditor will complete the audit and in what order. Normally this section would come closer to the top of the report before the results section." – (This is why it should be included, the below is an example of what it may look like in a real audit report.)

For the purposes of this audit, the auditor will complete the audit tasks in the following order. This will not change unless approved by the appropriate authority. The auditor will start will reviewing and auditing the polices and than to the different parameters listed below.

1. Logging Policy
2. Password Policy
3. BYOD Policy
4. Connection Settings
5. Configuration Settings
6. Installed Features
7. System Performance
8. Security Protocols

The auditor will than consult with any technical staff to ensure that there is nothing missing from the audit plan before completing the audit and starting the compilation of the final Audit Results. Once the auditor has competed the final results section of the report, the report will be submitted to the appropriate authority in the company managing the network router.

Control Procedures

An audit report should also have a section in place in the event of a delay or an unforeseen error or issue. This would be the control procedures section of the report. This section will go over what the auditor or technical staff assisting with the audited would do in the event of an issues such as a critical failure or something along those lines. An example of how to report an issue or record an error should be included to ensure that anyone that may create an error report follows the same guidelines.

References

There are no sources in the current document.

I referenced writing this report from my knowledge of writing an audit plan/report over the summer during my work-term.