IT SECURITY AUDIT REPORT

A picture containing outdoor object, wire, close

Description automatically generated

**APRIL 1, 2023**

XYZ Corp. – IT SECURITY AUDIT REPORT

DATDA

Table Of Contents

[Purpose of the Audit 3](#_Toc132459615)

[Scope of the audit 3](#_Toc132459616)

[Audit Summary 3](#_Toc132459617)

[Audit information 3](#_Toc132459618)

[Audit Summary 3](#_Toc132459619)

[Method of performing the audit. 3](#_Toc132459620)

[Strong Areas identified. 3](#_Toc132459621)

[Weak areas identified. 4](#_Toc132459622)

[ACTION PLAN 4](#_Toc132459623)

[Appendixes 4](#_Toc132459624)

[Appendix-A 4](#_Toc132459625)

[Appendix- B 4](#_Toc132459626)

[Finding- 1 4](#_Toc132459627)

[Recommendations 4](#_Toc132459628)

[Finding- 2 5](#_Toc132459629)

[Recommendations 5](#_Toc132459630)

[Finding -3 5](#_Toc132459631)

[Recommendations 5](#_Toc132459632)

[Finding-4 5](#_Toc132459633)

[Recommendations 5](#_Toc132459634)

[Finding-5 6](#_Toc132459635)

[Recommendations 6](#_Toc132459636)

[Conclusions 6](#_Toc132459637)

[FEEDBACKS: - 6](#_Toc132459638)

[References: - 7](#_Toc132459639)

# Purpose of the Audit

This report is based on the findings which outlines the IT audit conducted on XYZ Corp. The audit was done on 1-04-2023 with the cooperation of management and staffs of the XYZ corp. The aim was to identify and assess the effectiveness of the Security Controls of the Company and to find any possible threats or flaws in the working environment.

# Scope of the audit

The audit done for XYZ Corp focused mainly on the physical security, patch management, user access control, backup configurations, disaster recovery plan, password policy requirements.

# Audit Summary

## Audit information

In an overview, our assessment has finalised that XYZ Corp has implemented certain safety measures to protect the confidentiality, Integrity and Availability of the data and the networks. However, through our deep analysis and testing we must recommend some areas of improvement that could enhance the proper working environment and prevents from operational failures. Our report outlines the findings and remediation methods to address the issues and flaws.

## Audit Summary

### Method of performing the audit.

The audit was done with the globally accepted IT audit standards following the rules and regulations. We have executed the audit by personally interviewing the management and staffs and the authorised and examined their documents and accomplished various tests.

### Strong Areas identified.

We have identified that CCTV cameras are functioning properly, and access controls are performing the duties effectively to prevent unauthorised actions. We have reviewed the disaster recovery plan and back up mechanisms which are implemented by XYZ Corp met the standard regulations. The enforcement of security policies is done in a well manner and regular review is happening which is very important for the information security. Overall XYZ Corp has an efficient Infrastructure which boosts the productivity of employees. Another excellent practice observed is the regular cyber security training for the employees and maintenance of compliance.

### Weak areas identified.

Through our deep analysis, we have observed certain risk factors of the XYZ Corp which could possibly pave way for threats and disasters. The patch management is not regularly monitored, and we have observed some systems are found to be in the risk of critical vulnerabilities. The interior monitoring of the CCTV is placed effectively and the surveillance to the exterior should be added by placing a more high-resolution night vision supporting cameras with a high picture quality. The password policies should be further strengthened for better security by increasing the complexity and lockout duration. We have uncovered that there is no proper reviewing of identity management in revoke the access of discharged/relieved employees.

# action plan

The audit was done by using globally recognized standards and by properly reviewing the documents and data provided by XYZ Corp.

# Appendixes

## Appendix-A

This audit is conducted by Group-3 Security which is a professional and experienced company which provides cyber security services and auditing both internally and externally. We have a group of highly qualified and skilled candidates which holds the certificates of offensive security, CEH, and CISSP. We provide a clearly drafted report and have more than hundreds of trusted clients from all over the world. We assist to strengthen the security posture by deep analysing of the risks and provides assistance in remediation.

## Appendix- B

### Finding- 1

Administrative accounts are being used with generic user accounts which makes the auditing process complex and reduces accountability.

### Recommendations

The administrators should be refrained from using generic accounts and they should be assigned role based administrative access.

### Finding- 2

We have observed that XYZ Corp has enabled backups on data according to the severity. The critical data is incrementally backed up every day and those data that is not much critical is handled by a separate backup methodology.

### Recommendations

The severity-based data backup is having both benefits and added risks. As an immediate step, all the data backups should be made daily, and the backup mediums must be kept outside the premises to overcome natural disasters.

### Finding -3

The antivirus systems are consuming large system loads and it is affecting the workability of the employees. The traditional antivirus system is not capable of handling the modern threats and the patch management is consuming time and effort. Dedicated employees are working off times to push the antivirus patches to the systems as it created huge manual efforts and at the same time delivering patches over to the remote networks during off hours makes it complicated to the client systems to get it effected.

### Recommendations

Antivirus system should be upgraded in a medium-term plan. The new solution should include cloud-based antivirus updates and patch delivery. It will reduce the human effort and management huddles.

### Finding-4

The CCTV systems can do the job. The AI based recordings are making it effective. Motion sensor-based recording is Saving HDD space to around 80%. The backups are maintained to till 90 days. This meets the industry recommendations and standards. Access controls systems and the CCTV systems are time synced and the monitoring is happening normally, but it is noticed that XYZ corp still uses proximity cards for punching systems and access control systems to the key locations like datacenter, locker room etc.

### Recommendations

We have notices blind spots in certain critical areas in the organizations where the cash transactions are happening. These unsounding’s should be monitored with more cameras added. The in and out of vehicles to the premises are marked manually by the security staff and this should be automated by automatic number plate recognition system (ANPR)

The use of proximity card increases the risk of being it swapped by the employees. In a long run, the usage of proximity cards needs to be avoided. Instead, facial recognition system or biometric system should be included. This will improve the effectiveness of access control system.

### Finding-5

We have noticed that the fire protection system is not well maintained and only fire cans are observed there which can only be triggered manually.

### Recommendations

It is recommended that the data center should have fire fighting system to tackle fire related risks. The cooling system should be upgraded using centralized cooling unit (CCU) that has remote monitoring facility. The number of manually operated fire extinguishers should be added and automated system to tackle fire should be implemented.

# Conclusions

Overall, our audit uncovered the potential threats and flaws in the working of XYZ Corp which would impact the confidentiality, Integrity and Availability of the data and networks. Though, the findings and areas of improvement are mentioned which would enhance the workings and provides security to the systems including measures of fail-over. We highly recommend the Board of directors of XYZ Corp to immediately take actions to the directed issues and ensure the proper operations of the company.

# feedbacks: -

*< space for feedback >*

# References: -

* *IS Audit Basics: The Components of the IT Audit Report*. (n.d.). ISACA. Retrieved April 15, 2023, from <https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/is-audit-basics-the-components-of-the-it-audit-report#:~:text=It%20typically%20includes%20a%20high>
* *What is IT audit (information technology audit)? - Definition from WhatIs.com*. (n.d.). SearchCIO. <https://www.techtarget.com/searchcio/definition/IT-audit-information-technology-audit#:~:text=An%20IT%20audit%20is%20the>