

**IT AUDIT REPORT**

**April 2019**

**Table of Contents:**

[I. Executive Summary](#_Toc501013901)

* [Introduction](#_Toc501013902)
* [Background](#_Toc501013903)
* [Objective and Scope](#_Toc501013904)
* [Audit Approach](#_Toc501013905)
* [Summary of Findings](#_Toc501013907)

[II. Detailed Observations & Recommendations](#_Toc501013908)

* CONTROLS
* LACKING CONTROLS

III[. Appendix I](#_Toc501013910)

I[V. Appendix II](#_Toc501013911)

[V. Conclusion](#_Toc501013909)

[VI.](#_Toc501013911) Acknowledgment

1. Executive Summary:

Introduction:

This Audit for Bitco Investments as a part of the IT Audit Plan 2019. The overall engagement was planned about three weeks. This document contains the Audit approaches and the findings deducted from the Auditing of Bitco Investments. It also documents the controls that Bitco Investments lack and should change given the recommendations in the Auditing process.

Background:

The Bitco Investments is an American Digital Asset Trading Platform founded in 2017.

Bitco Investments are a team of experienced professionals who have previously founded successful companies which employ over 100 people, have raised over $60M in venture capital, and have achieved over $25M in annual revenue. The company now bring our experience of operating companies and building scalable technology to the world of digital assets.

We believe decentralized, non-custodial exchanges are the future of trading cryptocurrencies. It majorly deals with PII (Personally Indentifable Information) and PCI-DSS (Payment Card Industry-Data Security Standards).

Objective and Scope:

The objective and scope of IT Service Management Audit includes review of the following:

* Information Security Policy
* Password Management Policy
* Data Backup Policy
* User Access Management
* Network Security Policy
* Business Continuity and Disaster Recovery Policy
* IT Change Management Policy

Audit Approach:

Bitco Investments adopts a risk-based audit approach. In this context the key stages in our approach are as follows:

**Audit Planning**

* Initial meeting with the process owners to gain a broad understanding of business process and functions.
* The audit charter which identifies Responsibility, Authority and Accountability, Business risks and Due Dates that needs to be approved.
* Identify controls to manage/mitigate business risks.
* Discuss gaps and improvement options with Management team.

**Risk Assessment and Business process analysis**

* This will enable us to develop an overall and effective IS Audit plan which will consider all the potential weaknesses and /or absence of Controls and determine whether this could lead to a significant deficiency or material weakness.

**Performance of Audit Work**

* Requires us to provide supervision, gather audit evidence and document our audit work such as establishing an internal review process, obtain relevant evidences, observation and describing audit work done.

**Reporting**

* State the scope, objectives, period of coverage, nature, timing and the extend of the audit work
* State findings, conclusions, recommendations and any reservations, qualifications and limitations
* Provide audit evidence

Summary of Findings:

A summary of the findings noted during our audit review is given below. Our detailed observations and suggestions for improvement are included in the following sections of this report. To enable management set priorities on their action plans, we have reported our findings in two categories: High and Medium

Please find below a summary of our Observations which are sorted in the same order as outlined in the following sections of this report relating to detailed observations and recommendations along with management's planned actions:

|  |  |  |
| --- | --- | --- |
| **Sr.No.** | **Missing Control** | **Importance Level** |
| ­ |  |  |
| 1 | User access revocation delay | **High** |
| 2 | Absence of change log review | **High** |
| 3 | Failure to test the application changes in Testing environment | **High** |
| 4 | Unsatisfactory Password configuration requirements | **Medium** |

1. DETAILED OBSERVATIONS & RECOMMENDATIONS

Lacking Controls:

1. User Access revocation delay: **High importance**

|  |  |  |
| --- | --- | --- |
| **Area** | **Description** | **Recommendations** |
| Access Security revocation delay | Delay of 30 working days in the deactivation of user account of exited employee (Mr. Michael)   Some transactions of $10,000 were posted between 1/12/2019 to 01/21/2019 using user account “rmichael” after relieving date of Mr. Michael on 01/12/2019 as per HR exit list. | • Adhere to User Administration procedures for user creation / deletion, role modification / deletion and assignment / deletion of profiles. • Ensure User ID of resigned/separated employees (both on-roll and contract employees) must blocked/delete on or before last working day |
|
|
|
|
| **Management Comments** | | |
| Management will conduct the internal investigation about the delay in deactivation and financial transaction posting and will provide their report to Auditors and Compliance team by end of May 2019. | | |

1. Absence of change log review: **High importance**

|  |  |  |
| --- | --- | --- |
| **Area** | **Description** | **Recommendations** |
| Change log review | Management was unable to demonstrate on the change log review process performed for SWA application during the audit period.  Change log review report for SWA application during the audit period was not available.  The absence of change log review process increases likelihood of unauthorized changes being introduced to key business systems. | Adhere to IT Change Management policy and procedure to ascertain the change log reviews are conducted on regular basis. |
|
|
|
|
| **Management Comments** | | |
| Management will enforce the control to conduct the change log reviews on periodic basis and will submit the change log review report for audit period to Auditors and Compliance team. | | |

1. Failure to test the application changes in Testing environment: **High importance**

|  |  |  |
| --- | --- | --- |
| **Area** | **Description** | **Recommendations** |
| Change Testing | The management was unable to demonstrate the sample changes were tested in test environment prior moving into production environment. | Adhere to change testing policy and procedure to ascertain that they are followed in the environment. |
|
|
|
|
| **Management Comments** | | |
| Management will enforce the control to make sure that all the test cases will be reviewed and approved before moving into production on a periodic basis and submit the sample cases after the change has been implemented during the period to Auditors and Compliance team. | | |

1. Unsatisfactory Password configuration requirements: Medium importance

|  |  |  |
| --- | --- | --- |
| **Area** | **Description** | **Recommendations** |
| Password Management | The Management was unable to ascertain that the password management procedure is followed. The password expiry duration and account lockouts due to failed attempts to login is not working in some test cases. | Update the AD in the AWS to adhere to the password management policy. |
|
|
|
|
| **Management Comments** | | |
| Management will enforce controls to make sure that password management will be adhered to and also will be reviewed in a periodic basis. | | |

1. APPENDIX I

Overall grading guide is as follows:

**Satisfactory**

Indicates that the control environment is strong and indicates that Management effectively identifies and controls all major types of risks posed by the area / function under their responsibility.

**Generally Satisfactory**

Indicates that the control environment is sufficient to mitigate all high-risks related to the area / functions are being reviewed. While minor weaknesses exist, those have been recognized and are being addressed by Management.

**Improvements Required**

This indicates that the internal control may be lacking in some important respects, particularly as indicated by continued control exceptions or by the failure to adhere to written policies and procedures. The risks associated with the internal control system could have adverse effects on the efficiency and effectiveness of operations if corrective actions are not taken by Management.

**Unsatisfactory**

This rating indicates a critical absence of effective internal controls to identify, monitor, or control significant risk exposures together with the existence of severe weaknesses or deficiencies in internal controls that can constitute an unsafe and unsound practice and possibly lead to significant losses or otherwise irregularities and misconduct. When audit reviews present this grading; it requires Management’s and the Audit Committee’s immediate attention and action.

1. APPENDIX II

Each finding is assigned with a risk rating. The rating is based on the risk’s potential impact, if unmitigated, and its likelihood of occurrence. This in turn assists Management in understanding the importance to remediate as follows:

|  |  |
| --- | --- |
| Risk Rating | Description |
| **High** | A key control objective is not met and poses a significant threat to the business. This finding anticipates the need for Management to address the issue with urgency to mitigate the adverse potential impact to the business. |
| Medium | An important control objective is not met and / or is a significant control weakness. This finding anticipates the need for Management to address the issue within a reasonable time-frame to maintain data integrity. |

1. CONCLUSION:

Our grading of the overall opinion is “Improvements required”, this indicates that the internal control may be lacking in some important respects, particularly as indicated by continued control exceptions or by the failure to adhere to written policies and procedures. The risks associated with the internal control system could have adverse effects on the efficiency and effectiveness of operations if corrective actions are not taken by Management.

(Please refer to Appendix I for grading definitions).

1. ACKNOWLEDGEMENT

We would like to express our gratitude to the management for their assistance and cooperation.