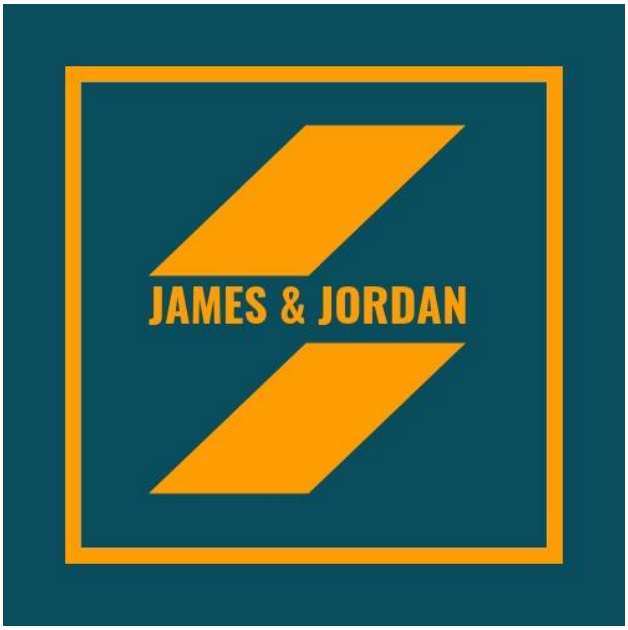

JAMES & JORDAN

Description of the organizational background relevant to Security, Availability and Confidentiality with the Auditor's report including detailed findings and recommendations conducted during November 3rd, 2018 to December 8th, 2018

For

Alpha Investments Inc.

CONTENT

EXECUTIVE SUMMARY

INTRODUCTION:

This audit for Alpha Investments Inc. was performed as part of the IT Audit Plan 2018. The overall engagement was planned about three weeks.

This IT audit engagement assesses the following areas:

- IT Service Management Policies and Procedures;
- User Access Management;
- Password Management;
- Performance Management;
- Incident Management
- Change Management;

BACKGROUND:

Alpha Investments Inc. is a Hedge Fund company based in Boston and founded in 2016. It aims at providing investment opportunities to the elite that are designed to protect investment portfolios from market uncertainty, while generating positive returns in both up and down markets.

Alpha Investments Inc. apply science and research to investment management. They evaluate stock trends with machine learning tools and artificial intelligence algorithms to understand the nature of the stock that helps investors make better informed choices and calculated risk decisions. All machine learning tools and artificial intelligence algorithms are developed in house by their data scientists and our exclusive only to the organization.

OBJECTIVE AND SCOPE:

Alpha Investment's cloud architecture will be tested through the collection and analysis of evidences based on criteria in SOC2 which follows the CIA (Confidentiality-Integrity-Availability) principle. There will be a clear and unambiguous conclusion based off the grading criteria mentioned in *Appendix 3: Grading Guide*. The Audit assesses the IT processes, practices, and controls and are filled in SOC 2 control worksheet. The audit

results were used to make sure every component of cloud architecture and IT management is in control.

The process is as follows:

- Research company policies, procedures and background at the beginning of the audit
- Onsite system check and documentary examination of where evidence of completeness and/or validation (existence) is required
- Interview stakeholders and employees

Those components are monitored and updated regularly to achieve Alpha Investment's business goal. The integrity of the system is maintained while following the compliance of law regulation and contractual agreements to which the business prospects are subjected.

The scope of this audit is focused primarily on the Alpha Investment's cloud architecture where information is transferred between user and the service application. The audit was done between November 3rd, 2018 and December 8th, 2018 for all the departments within the organization. This includes scrutinizing internal controls for Confidentiality, Security and Availability principles.

AUDIT APPROACH:

James & Jordan adopts a risk-based audit approach. In this context the key stages in our approach are as follows;

- Use SOC 2 control worksheet to audit IT practices, cloud processes and controls
- Gather evidences from IT controls and processes to assess Alpha Investment's current state and principles
- Review control evidences in accordance with the SOC 2 worksheet and conduct interviews

ACKNOWLEDGEMENT:

We would like to express our gratitude to the entire management and the employees at Alpha Investments Inc. for their assistance and cooperation.

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.	Specifics	Risk Rating
1.	Easy to navigate Incident Report fully exhibiting incident facts is missing	Medium
2.	Absence of timely de-provisioning of user access to data and organizationally-owned or managed applications, infrastructure systems and network components	High
3.	Risk assessment plan and treatment procedures are in place and retained but assessment meetings are not conducted	Medium
4.	Absence of Change Log Review and Update	High

DETAILED OBSERVATIONS AND RECOMMENDATIONS

Observation 1

Audit Criteria:

CC6.2: Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.

Findings: Easy to navigate Incident Report fully exhibiting incident facts is lacking

Analysis:

When an incident occurs in a system, details of the incident need to be documented in a report and sent over to senior managers responsible for immediate or later review. With regards to the importance of an incident report, it can provide controls aiming at recording

objective facts, detecting and discovering unwanted events, making corrective decisions and analyzing lessons to be learned.

The 10 essential elements of an incident report are ‘specific details and description’, ‘facts only’, ‘objective tone’, ‘organisation’, ‘witness statements’, ‘confidential concerns’, ‘accuracy’, ‘good grammar’, ‘sketches, diagrams and photos’, and ‘supervisor signature’

The incident reports that Alpha Investments provided had specific details and descriptions about the incident facts; incident reports were written in good grammar, witness statements were quoted, supervisor signatures had been included on the last pages of the reports. However, auditors still found several components needed to be improved, which resulted the overall procedure as ‘unacceptable’ in the audit.

- Not easy to locate a specific incident report by searching a keyword
- Possible confidential information found (login information)
- No screenshots, only Narratives

Risk:

Incidents occur frequently in the workplace. Accidents and events, both minor and major, can occur without any immediate or apparent effect on property or people, but can have substantial physical or financial impacts down the track. Failure to include important information, can stunt the ability of the person responsible to resolve the issue and limit the usage of resources at his disposal just because he does not have enough information.

Capturing all information about incidents, not just the reportable one, can also help reduce risk and prevent future incidents. The reporting of a near miss is a great way to highlight how valuable the process can be.

Recommendation:

- Auditors recommended that management index the incident reports chronologically with clear subheadings.
- Avoid referring confidential data in the reports.
- Recommended adding screenshots to make incidents easy to recall and more understandable.
- More information such as time stamps can be added to sort the reports.

Management Response:

Agree. Meeting has been held to discuss about retention of the incident reports. Relevant persons in charge have been assigned to the task within the organization. Reports are labelled and sorted chronologically for convenience of search. Diagrams and screenshots will be added wherever necessary. Time frame: 1 month

Observation 2

Audit Criteria:

CC5.2: New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

Findings: Absence of timely de-provisioning of user access to data and organizationally-owned or managed applications, infrastructure systems and network components

Analysis:

Account deprovisioning is the account of removing an employee's credentials, such as company email, account access, computer access, and other things.

Timely revocation or termination of user access to any organizational component must be implemented based on established Policies and Procedures and on user's status change (change of department, employment termination, contract expiration). Management provided a list of all user accounts and active accounts with designated permission matrix however, failed to present documentation listing former employees/contractors and their access capabilities.

Risk:

Deprovisioning is a very important aspect when it comes to managing employees, especially upon termination. Not only is it just good for organization and keeping track of current and previous employees, but it's a security measure. There are several cases in which former and disgruntled employees have been able to get back into a company via their own credentials or have figured out ways in which to skirt around them.

Recommendation:

- Management was recommended to conduct a periodic evaluation of Access control procedures (*See Appendix 2: Standard Operating Procedures*)
- Document users who are both functional and nonfunctional within the organization
- Have access of terminated entities revoked with immediate effect

Management Response:

Agree. Management has drawn up a procedure to record and retain information on user's whose access has been revoked in the past. They have asserted the records will be reviewed and updated as and when necessary, every 6 months.

Observation 3

Audit Criteria:

CC3.2: The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.

Findings: Risk treatment plan is in place and retained but Risk assessment meetings are not conducted.

Analysis:

A risk assessment is not only an important step in ensuring a safe and healthy work environment, it is a legal requirement. It needs to be conducted before employees' complete work on current processes and start something new. Organizations must consider the possible causes of the risk and what steps to take in preventing the harm in the first place.

With Alpha Investments, the senior executives talked about their Risk Management plan where a designated Risk Assessor would review the issues in question and come up with a solution within the scope of the organization based on their established operating procedure. However, when asked, the executives were unable to furnish the evidences for e.g. minutes from the meetings held or a comprehensive risk assessment report to support their claim.

Risk:

- Not having an accurate risk assessment process in place puts an organization at risk of not being able to handle unknown, hidden, undetected or unrelated risks causing more uneasiness

- Without a solid risk assessment procedure, a person cannot choose which preventive/corrective practice measure is most appropriate to use
- Risk cannot be managed or addressed unless it is first identified

Recommendation:

Recommended management to conduct a risk assessment meeting, on a monthly basis, in order to, among others, assess the risks identified and come up with a viable solution

Management Response:

Agree. Management will conduct meetings noting that they addressed (minutes), among others, the risk assessment aspects and the action items in accordance with the Risk Treatment plan.

Observation 4

Audit Criteria:

CC7.4: Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and confidentiality commitments and system requirements.

Findings: Absence of Change Log Review and Update

Analysis:

Change control aims at ensuring that a systematic approach is taken to making configuration changes to IT systems and the company infrastructure on a whole. Absence of Change control disrupts critical line-of-business systems. Change control is facilitated through Change Control Requests (CCRs) which document proposed changes, shows that they've been tested, outlines the potential risks of making the change and provides a rollback plan should there be unexpected issues.

However, these CCRs can come in for a major or minor change which will affect the organization accordingly. To assess their importance further down the line, it is important to have an evaluation review process in place for the change requests that come in. Conducting these reviews will ensure that everyone is on the same page and responds to change requests unanimously.

Alpha Investment's policy structure does not address the importance of a Change log. The absence of this element in the Change control management would make it impossible

to respond to the transformation requirements on a timely and a reliable basis in an efficient way to use company resources.

Risk:

The absence of change log review process increases likelihood of unsuitable changes being introduced to key business systems.

Recommendation:

Auditor recommended that management adhere to IT Change Management policy and procedure to include and ascertain the practice of updating Change logs and reviewing them on regular basis.

Management Response:

Agree. 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.

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 3: Grading Guide* for grading definitions).

APPENDIX 1: POLICIES

1. ACCESS CONROL POLICY
   How is access to and control of the storage, virtualization and network infrastructures managed? What protocols are in place for monitoring, granting access and logging changes to client information systems?

2. INFORMATION SECURITY MANAGEMENT POLICY
   What safeguards does the provider have in place to protect against physical and virtual threats? How are security violations and incidents reported and managed? What information does the provider collect about clients and how is it handled? Has the provider ever had a security breach, and if so, what was the outcome?

3. EMPLOYEE AND CONTRACTOR PHYSICAL SECURITY POLICY
   What practices are in place for monitoring employees, visitors and contractors while on premise (office or data center)? What background verification, screening agreements and employment agreements are established?

4. CHANGE CONTROL POLICY
   Formal process for making changes in the company or to the IT systems and services

5. RISK ASSESSMENT AND MANAGEMENT POLICY
   The process of identifying, analyzing, treating and monitoring the threats and risks associated with them.

6. CONFIDENTIALITY POLICY
   The purpose of the Confidentiality Policy is to ensure that all staff, members, volunteers and users understand the Organization's requirements in relation to the disclosure of personal data and confidential information.

7. DISASTER RECOVERY POLICY
   Area of security planning that aims to protect an organization from the effects of significant negative events.

APPENDIX 2: PROCEDURES

1. Access Enforcement per Separation of Duties
2. Data breach procedure and Response plan
3. Visitor/Non-visitor permissions for company assigned contractors and personnel
4. Completing a Change Control Request (CCR) form
5. Assessing risk impact and developing risk treatment plan
6. Signing a non-disclosure agreement
7. Contingency plan for business continuity

APPENDIX 3: GRADING GUIDE

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 enough 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.

APPENDIX 4: RISK RATING

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	Description	Priority
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.	1
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.	2

APPENDIX 5: TEST PROCEDURES

Domain	Risk	Control Criteria	Testing procedure	Test Result
IT Risk Management Framework	Lack of a Risk Management Framework may lead to undetected impact of the IT risk on the business. This may result in strategic, operational, financial and legal issues.	CC3.2: The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	• Verify whether an IT risk assessment has been performed and mitigation strategies have been implemented and are monitored. • Verify that IT risk management is regularly reported to executive management and Board of Directors.	Minimal deviations noted.
User account management	Ineffective user account management increases the risk of unauthorized to data. This may lead to information theft, loss of data integrity, potential fraud, and breach of confidentiality.	CC5.2: New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	• Obtain a list of terminated employees during the period under audit. • Determine if access had been removed or deactivated timely from the systems in-scope. • Obtain the report of user access review and verify that appropriate action has been taken for unauthorized/ inappropriate users.	Deviations noted.
Change management	If changes are not reviewed in a periodic basis there is an increased risk that unauthorized or inappropriate changes will not be identified and	CC7.4: Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and	• Enquire with appropriate staff to ascertain that management reviews changes on periodic basis. • Obtain the report/ results of change reviews	Deviations noted

	resolved in a timely matter.	confidentiality commitments and system requirements.		
Information Security and Privacy management	If incident reporting is not optimized, there is an increased risk that unauthorized or inappropriate system actions, such as deleting or modifying sensitive data, or access attempts will occur and will not be identified and resolved in a timely matter.	CC6.2: Security, availability, and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	• Select a sample of problems/incidents and validate that they were resolved in a timely manner, as per policy. • Enquire about specific incident reports within a given time period.	Minimal deviations noted.