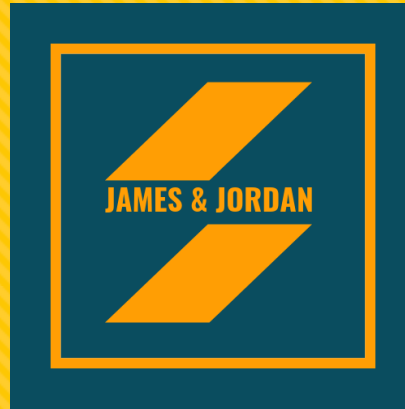


ALPHA INVESTMENTS INC



AUDITED BY : JAMES & JORDAN LLC

GROUP MEMBERS:

RISHI RAJ RAJANI, GAURESH CHAVAN, KAUSHAL CHAUDHARY,
MOHIT RUKE, RISHI RAJ DUTTA, ZEXU HUANG

EXECUTIVE BACKGROUND

- Hedge Fund company based in Boston
- Founded in 2016
- **Goals:** Provide investments opportunities to the elites and solutions to get good returns
- Evaluate ML and AI algorithms to understand the stock market nature and understand when to invest in a particular stock to get maximized returns

OBJECTIVE OF THE AUDIT

- Assess and evaluate different processes to safeguard company assets using following processes:
 - IT Service Management Policies and Procedures
 - User Access and Password Management
 - Performance Management
 - Incident Management
 - Change Management

SCOPE OF THE AUDIT

- Testing of **ALPHA INVESTMENTS INC** cloud architecture
- Collection and Analysis of evidences mentioned in the SOC2 report
- Assessment of the IT processes, practices and controls
- Observing key findings and giving recommendations
- Determining the result based on the grading criteria to ensure whether the company's policies are in place

AUDIT APPROACH

- Organize a meeting with the executives
- Identify business risks
- Identify controls to manage/mitigate business risks
- Collect Evidences
- Discuss gaps and improvement options with Management team
- Agree Management Action Plan, Responsibility & due dates

KEY FINDINGS

AREA	RISK RATING
Disaster Recovery	Medium
Access Control	High
Risk Assessment & Treatment	Medium
Change Control	High

DISASTER RECOVERY

- Easy to navigate, safe to use Incident Report fully exhibiting incident facts is lacking
- **Auditor's Recommendations:**
 - Indexing Incident Reports chronologically with subheadings
 - Avoid inclusion of confidential data in the reports
 - Addition of screenshots to make incidents easy to recall and understandable
 - Addition of Timestamps to sort the reports
- **Management's Response:**
 - Organized a meeting to discuss about retention of incident reports
 - Assigned a Person in charge to take care of this situation
 - Agreed to include proper documentation and screenshots wherever necessary

ACCESS CONTROL

- Absence of timely de-provisioning of user access to data and organizationally-owned or managed applications, infrastructure systems and network components
- **Auditor's Recommendations:**
 - Recommendation of conducting periodic evaluation of Access Control Procedures
 - Document user access controls of former employees with immediate effect
- **Management's Response:**
 - Agreed to record and document information of users whose access has been revoked
 - Asserted the records to be reviewed and updated every 6 months

RISK ASSESSMENT

- Risk assessment plan and treatment procedures are in place and retained but assessment meetings are not conducted
- **Auditor's Recommendations:**
 - Conduct Monthly Risk Assessment meeting with the person in charge
 - Assessments of the identified risks and provide appropriate solutions
- **Management's Response:**
 - Agreed to conduct monthly meetings and record the meetings in the calendar as an evidence
 - Address the risks and come up with a mitigation plan

CHANGE CONTROL

- Absence of Change Log Review and Update
- **Auditor's Recommendations:**
 - Adhere to IT Change Management policy and procedures
 - Conduct reviews on Log change
- **Management's Response:**
 - Agreed to enforce the control to conduct the change log reviews on periodic basis
 - Agreed to submit change log review report for audit period to Auditors and Compliance team

GAP ANALYSIS

CURRENT STATE	IDEAL STATE	GAP	ACTION PLAN
Company failed to provide specifics about the occurred incidents	Incident Reporting adhering to Disaster Recovery Policy	Missing evidences for incident reports	Periodic meetings conducted for the retention of incident reports
Company does not have deprovisioning procedures in place for former employees	Timely revocation or termination of access under User Access Management	Former Employees data missing	Current and Former employees data perfectly documented
Company failed to provide details about the risk assessment meetings	Risk Assessment procedures in accordance with Risk Treatment Procedures	No evidences of assessments being conducted	Monthly Risk Assessment meetings conducted to identify and mitigate risks
Company policy structure does not address the importance of a Change log	Reviewing and updating change log under Change Control Management Policy	Absence of Change Log Review and Update	Making reports of the change log review periodically

CONCLUSION

- Overall Grading : Improvements required
- Failed to provide documented evidences for some important controls
- 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