BI HELPER

System and Organization Controls (SOC) 2 Type II

Report on management's description of the BI Helper software application and the suitability of the design and operation of controls for its security, availability and confidentiality

For the period from October 1, 2023 to March 31, 2024

Table of Contents

I Assertion of BI Helper Management

We have prepared the accompanying description of the BI Helper Software Application (BI Helper) for the period from October 1, 2023 to March 31, 2024 based on the criteria for a description of a service organization's system in DC section 200, *2018 Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*. The description is intended to provide report users with information about the BI Helper Software Application that may be useful when assessing the risks arising from interactions with BI Helper's system, particularly information about system controls that BI Helper has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

BI Helper uses subservice organizations to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at BI Helper, to achieve BI Helper's service commitments and system requirements based on the applicable trust services criteria. The description presents BI Helper's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of BI Helper's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at BI Helper, to achieve BI Helper's service commitments and system requirements based on the applicable trust services criteria. The description presents BI Helper's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of BI Helper's controls.

We confirm to the best of our knowledge and belief that:

1. The description presents the BI Helper Software Application that was designed and implemented throughout the period from 10/1/2023 to 3/31/2024 in accordance with the description criteria.
2. The controls stated in the description were suitably designed through the period from 10/1/2023 to 3/31/2024 to provide reasonable assurance that BI Helper's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of BI Helper's controls throughout that period.
3. The controls stated in the description operated effectively through the period from 10/1/2023 to 3/31/2024 to provide reasonable assurance that BI Helper's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of BI Helper's controls operated effectively throughout that period.

Signed by BI Helper Management
<Kiran Hosakote>

II Description of the BI Helper Software Application

Types of Services Provided

The BI Helper software application is a cloud-hosted platform for automated distribution of business reports. Any other services provided by BI Helper are not in the scope of this report.

Principal Service Commitments and System Requirements

BI Helper designs its processes and procedures to meet objectives for its software application. Those objectives are based on the service commitments that BI Helper makes to customers and the compliance requirements that BI Helper has established for their services.

Security commitments to user entities are documented and communicated in BI Helper's customer agreements, as well as in the description of the service offering provided online. BI Helper's security commitments are standardized and based on common principles that include but are not limited to:

1. The fundamental design of BI Helper's software application addresses security concerns such that system users can access the information based on their role in the system and are restricted from accessing information not needed for their role.
2. BI Helper implements various procedures and processes to control access to the production environment and the supporting infrastructure.
3. Monitoring of key infrastructure components is in place to collect and generate alerts based on utilization metrics.

BI Helper establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in BI Helper's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal networks are managed and how staff are hired.

Components of the System used to provide Services

Infrastructure

The production infrastructure for the BI Helper software application is hosted on Amazon Web Services (AWS) in their US East (North Virginia) region. AWS is a secure cloud services platform, and their physical infrastructure is accredited under ISO 27001, SOC 1, SOC 2, PCI Level 1 and CSA Star.

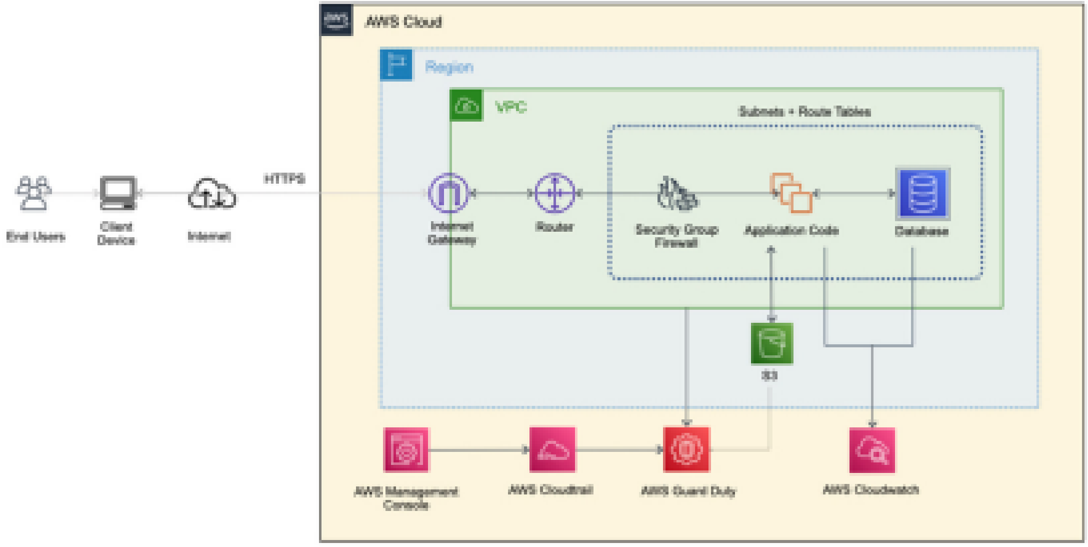
Network Architecture

BI Helper software application uses a virtual and secure network environment on top of AWS infrastructure to ensure that the software application is always protected. This is achieved by hosting the application inside a virtual private cloud (VPC) and accompanying firewalls on the infrastructure provider. BI Helper software application ensures there are only specific authorized points of entry, and filters traffic to the private networks that support the application.

When a customer's client device connects to the application over the internet, their data is encrypted and secured over HTTPS. It then passes through an AWS Internet Gateway, over to a Virtual Private Cloud that:

1. Houses the entire application runtime
2. Protects the application runtime from any external networks

The internal networks of AWS are protected by deny-by-default security groups and firewalls to ensure that only deliberately allowed traffic can pass through. Further, all VPC network flow logs, DNS logs, and other AWS console events are continuously monitored by AWS GuardDuty to spot malicious activity and unauthorized behavior. Specifically, AWS GuardDuty uses machine learning, anomaly detection and integrated threat intelligence to identify potential threats.



Software

The BI Helper software application is hosted on Linux servers. The application has been programmed using Python and Java. All client data is stored in a MySQL database. For Identity and Access Management, logging and monitoring capabilities, as well as for providing authorization to the production environment, services offered by the infrastructure provider are used. BI Helper uses AWS Audit Manager to provide continuous compliance monitoring of the company's system.

People

BI Helper has a staff of five personnel organized into various functions and roles.

Senior Management: Senior management carries the responsibility for achieving the mission and objectives of the organization. They ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the organization's mission. They also assess and incorporate results of the risk assessment activity into their decision-making process. Senior management understands that their support and involvement is required in order to run an effective risk management program that assesses and mitigates IT-related mission risks.

Information Security Officer: The Senior Management assigns the role of Information Security Officer to one of its staff members who is responsible for the performance of the information security function of the organization. Decisions in this area are based on an effective risk management program. The Information Security Officer is responsible for identifying risks, threats, vulnerabilities, and adding controls to mitigate this risk. Additionally, they also summarize remaining residual risks and report the same to Senior Management in a timely manner.

Compliance Program Manager: The company assigns the role of Compliance Program Manager to a staff member responsible for the smooth functioning of the Information Security Program. The Compliance Program Manager takes care of effective and timely completion of tasks required for the functioning of all information security controls, across all functions/departments of the organization.

System Users: The organization's staff members are the users of the IT systems. The organization understands that use of the IT systems and data according to an organization's policies, guidelines and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, staff members are provided annual security awareness training.

Procedures and Policies

Formal policies and procedures have been established to support the BI Helper software application.
These policies cover:

- Code of Business Conduct
- Change Management
- Data Retention
- Data Backup
- Information security
- Vendor management
- Physical security
- Risk management
- Password
- Media disposal
- Incident management
- Endpoint security
- Encryption
- Disaster recovery
- Data classification
- Confidentiality
- Business continuity
- Access control
- Acceptable usage
- Vulnerability management

All policies are made available to all staff members to provide direction on their responsibilities related to the functioning of internal controls. All staff members are expected to adhere to the policies and procedures that define how services should be delivered. Specifically, staff members are required to acknowledge their understanding of these policies upon hiring and annually thereafter.

BI Helper also provides information to clients and staff members on how to report failures, incidents, concerns or complaints related to the services or systems in the event there are problems, and takes actions within an appropriate timeframe as and when issues are raised.

Data

All data that is managed, processed and stored as a part of the BI Helper software application is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value and criticality to achieving the objectives of the organization.

Further, all customer data is managed, processed and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. All customer data storage and transmission follow industry-standard encryption. Data is regularly backed up as documented in the Data backup policy. Data backups are replicated across multiple regions to ensure it is available even in case of a local disaster.

Physical Security

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls of the in-scope system. BI Helper reviews the SOC 2 report provided by AWS on an annual basis, to ensure their controls are in accordance with standards expected by the customers of the BI Helper software application.

Logical Access

The BI Helper software application uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. User access, which is role-based, is controlled in the software application and authenticates to the database.

BI Helper has identified certain systems that are critical to meet its service commitments. All access to critical systems is under the principle of least required privilege (wherein a staff member is granted the minimum necessary access to perform their function) and controlled by the role of the staff member.

The Information Security Officer is responsible for performing periodic reviews of everyone who has access to the system and to assess the appropriateness of the access and permission levels and make modifications based on the principle of least privilege, whenever necessary.

Change Management

A documented Change Management policy guides all staff members in documenting and implementing application and infrastructure changes. It outlines how changes to the BI Helper system are reviewed, deployed and managed. The policy covers all changes made to the BI Helper software application regardless of their size, scope or potential impact.

The change management policy is designed to mitigate the risks of:

- Corrupted or destroyed information
- Degraded or disrupted software application performance
- Productivity loss
- Introduction of software bugs, configuration errors, vulnerabilities, etc.

A change to the BI Helper software application can be initiated by a staff member with an appropriate role. BI Helper uses a version control system to manage and record activities related to the change management process.

The version control system maintains source code versions and migrates source code through the development and testing process to the production environment. The version control software maintains a history of code changes to support rollback capabilities. It also facilitates the code review process which is mandated for all changes.

To initiate a change, the developer first creates a feature branch with the updated code. Once the code change is ready for review, the developer submits the code for peer review and automated testing, known as a pull request. For all code changes, the reviewer must be different from the author. Once a pull request is approved, the change can be released to production.

The ability to implement changes into the production infrastructure is restricted to only those individuals who require the ability to implement changes as part of their responsibilities. Further AWS CloudTrail is configured to track all changes to the production infrastructure.

Boundaries of the System

The scope of this report includes the BI Helper SaaS software application. It also includes the people, processes and IT systems that are required to achieve our service commitments toward the customers of this application.

BI Helper depends on a number of vendors to achieve its objectives. The scope of this report does not include the processes and controls performed by the vendors. The management understands that risks exist when engaging with vendors and has formulated a process for managing such risks, as detailed in the Risk Assessment section of this document.

III Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer and monitor them. Integrity and ethical values are essential elements of BI Helper's control environment, affecting the design, administration and monitoring of other components. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct.

BI Helper and its management team has established the following controls to incorporate ethical values throughout the organization:

- A formally documented Code of Business Conduct communicates the organization's values and behavioral standards to staff members.
- Staff members are required to acknowledge upon hiring (and annually thereafter) comprehensive policies and procedures covering the areas of Information Security, Change Management, Incident Management and Access Control. Staff members also acknowledge that they understand their responsibility for adhering to the policies and procedures.
- All new employees go through background checks as a part of the hiring process.

Commitment to Competence

BI Helper's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. The following controls have been established in order to incorporate the commitment to competence throughout the organization:

- Management outlines the roles and responsibilities of technical staff to ensure that they are clear about their responsibilities in the organization. These roles and responsibilities are reviewed annually by the senior management.
- Annual Security Awareness Training is provided to all staff which focuses on maintaining the security of the proprietary and customer-servicing systems and related data.
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of their job responsibilities.
- Employees are evaluated for competence in performing their jobs at the time of hiring.

Management Philosophy and Operating Style

BI Helper's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to monitoring business risks and management's attitudes toward personnel and the processing of information.

Specific control activities that the service organization has implemented in this area are described below:

- Senior management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Senior management reviews the functioning of internal controls, vendor risk assessment, risk assessment and high severity security incidents annually.

Organizational Structure and Assignment of Authority and Responsibility

BI Helper’s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs based on its size and the nature of its activities.

Management is committed to maintaining and improving its framework for how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. This also includes policies relating to appropriate business practices, knowledge and experience of key personnel and resources provided for carrying out duties.

In addition, it includes policies and communication directed at ensuring personnel understand the entity’s objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Organizational charts are in place to communicate key areas of authority and responsibility. These charts are accessible to all employees of the company and updated as required.

Human Resources Policies and Practices

BI Helper’s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity and ethical standards. The result of this success is evidenced by management’s ability to hire and retain top quality personnel who ensure the service organization is operating at maximum efficiency.

Specific control activities that the service organization has implemented in this area are described below:

- Employees are evaluated for competence in performing their jobs at the time of hiring.
- New employees are required to acknowledge company policy on hiring and re-acknowledge annually.
- Performance evaluations for each employee are performed on an annual basis.
- When a person is relieved of duties from the company, access to critical systems are revoked within 3 business days.

Risk Assessment

BI Helper’s risk assessment process identifies and manages risks that could potentially affect its ability to provide reliable services to its customers. The management is expected to identify significant risks inherent in products and services as they oversee their areas of responsibility. BI Helper identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels and implements appropriate measures to monitor and manage the risks.

This process identifies risks to the services provided by the BI Helper software application, and the management has implemented various measures designed to manage these risks.

BI Helper believes that effective risk management is based on the following principles:

1. Senior management's commitment to the security of BI Helper software application.
2. The involvement, cooperation and insight of all BI Helper staff.
3. Initiating risk assessments with discovery and identification of risks.
4. Thorough analysis of identified risks.
5. Commitment to the strategy and treatment of identified risks.
6. Communicating all identified risks to the senior management.
7. Encouraging all BI Helper staff to report risks and threat vectors.

Scope

The Risk Assessment and Management program applies to all systems and data that are a part of the BI Helper software application. The BI Helper risk assessment exercise evaluates infrastructure such as computer infrastructure, containing networks, instances, databases, systems, storage and services. The risk assessments also include an analysis of business/IT practices, procedures and physical spaces as needed. Risk assessments may be high level or detailed to a specific organizational or technical change as the stakeholders and technologists see fit.

Overall, the execution, development, and implementation of risk assessment and remediation programs is the joint responsibility of BI Helper's Information Security Officer and the department or individuals responsible for the area being assessed. All BI Helper staff are expected to cooperate fully with any risk assessment being conducted on systems and procedures for which they are responsible. Staff are further expected to work with the risk assessment project lead in the development of a remediation plan per risk assessment performed.

Vendor Risk Assessment

BI Helper uses a number of vendors to meet its business objectives. BI Helper understands that risks exist when engaging with vendors and as a result, continuously assesses those risks that could potentially affect the Company's ability to meet its business objectives.

BI Helper employs several activities to effectively manage their vendors. Firstly, the Information Security Officer performs an annual exercise of thoroughly examining the nature and extent of risks involved with each vendor relationship. For critical vendors, BI Helper assesses vendor compliance commitments through the review of available information security assessment reports and determines whether compliance levels adequately support BI Helper's commitments to its customers. If a critical vendor is unable to provide a third-party security report or assessment, BI Helper management meets with such vendors periodically to assess their performance, security concerns, and their services. Any vendor risks identified are recorded in the risk assessment matrix which is reviewed annually by the Senior Management of the company.

Integration with Risk Assessment

As part of the design and operation of the system, BI Helper identifies the specific risks that service commitments may not be met, and designs controls necessary to address those risks. BI Helper's management performs an annual Risk Assessment Exercise to identify and evaluate internal and external risks to the business as well as their potential impacts, likelihood, severity and mitigating action.

Monitoring

BI Helper management monitors controls to ensure that they are operating as intended and that the controls are modified as conditions change. Monitoring activities are undertaken to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Staff activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, independent evaluations or a combination of the two.

Information and Communication Systems

BI Helper maintains a company-wide Information Security Policy supported by detailed standards and training to ensure that employees understand their individual roles and responsibilities regarding security and significant events.

Further, BI Helper has policies and procedures that define access management, change management, and authentication requirements and procedures for critical systems. These policies and procedures are published and made available to internal staff.

Significant Events and Conditions

BI Helper has implemented automated and manual procedures to capture and address significant events and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with all relevant information for any impact to the software application.

Trust Services Categories

The following Trust Service Categories are in scope. **Common Criteria (to the Security, Availability and Confidentiality Categories).**

1. **Security** refers to the protection of:
    a. information during its collection or creation, use, processing, transmission, and storage.
    b. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction or disclosure of information.
2. **Availability** refers to the accessibility of information used by the entity’s systems, as well as the products or services provided to its customers. The availability objective does not in itself set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include

controls to support accessibility for operation, monitoring, and maintenance.

3. **Confidentiality** addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Any applicable trust services criteria that are not addressed by control activities at BI Helper are described within the sections titled **Complementary User Entity Controls** and **Complementary Subservice Organization Controls**.

Complementary Customer Controls

BI Helper’s controls cover a subset of overall internal control for each user of the software application. The control objectives related to BI Helper cannot be achieved solely by the controls put in place by BI Helper; each customer’s internal controls need to be considered along with BI Helper’s controls. Each customer must evaluate its own internal control to determine whether the identified complementary customer controls have been implemented and are operating effectively.

Complementary Customer Control List	**Related Criteria**
Customers are responsible for managing their organization’s BI Helper software application account as well as establishing any customized security solutions or automated processes through the use of setup features.	CC5.1, CC5.2, CC5.3, CC6.1
Customers are responsible for ensuring that authorized users are appointed as administrators for granting access to their BI Helper software application account.	CC5.2, CC6.3
Customers are responsible for notifying BI Helper of any unauthorized use of any password or account or any other known or suspected breach of security related to the use of BI Helper software application.	CC7.2, CC7.3, CC7.4

Customers are responsible for any changes made to user and organization data stored within the BI Helper software application.	CC8.1
Customers are responsible for communicating relevant security and availability issues and incidents to BI Helper through identified channels.	CC7.2, CC7.3, CC7.4

Complementary Subservice Organization Controls

The BI Helper software application utilizes AWS to provide cloud infrastructure. AWS is responsible for operating, managing and controlling the underlying infrastructure components supporting the services which are utilized by the BI Helper software application.

BI Helper’s Information Security Officer is responsible for reviewing audit reports performed by independent auditors of AWS for security considerations.

Controls expected to be implemented at AWS	**Complemented Criteria Ref. Number**
● Password and/or MFA is used to restrict access to authorized individuals. ● Encryption methods are used to protect data in transit and at rest. ● Roles and responsibilities for managing cryptographic keys are formally documented. ● Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters. ● Network communications within a VPN Gateway are isolated from network communications within other VPN Gateways. ● Security protections are in place to restrict access to virtual and physical devices and other information assets to authorized personnel.	CC6.1
● Additions and changes to systems are authorized prior to access being granted. ● System access is removed timely upon termination.	CC6.2

● System access is removed timely upon termination. ● System access is reviewed on a periodic basis to ensure access is restricted to authorized and appropriate individuals. ● IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning.	CC6.3

● Only authorized personnel have access to the facilities housing the system. ● Badge access control systems are in place in order to access the facilities. ● Visitor access to the corporate facility and data center are recorded in visitor access logs. Visitors are required to wear a visitor badge while onsite at the facilities. ● Visitors are required to check in with security and show a government issued ID prior to being granted access to the facilities. ● Visitors are required to have an escort at all times.	CC6.4
● All production media is securely decommissioned and physically destroyed prior to leaving the data center.	CC6.5
● Customer-facing websites are secured with HTTPS, and the websites' TLS certificates are tracked and renewed in advance of their expiration.	CC7.1
● Changes are authorized, tested, and approved prior to implementation.	CC8.1
● Environmental protections have been installed including the following: ○ Cooling systems ○ Battery and generator backups ○ Smoke detection ○ Dry pipe sprinklers ● Environmental protection equipment receives maintenance on at least an annual basis.	A1.2
● Backups of critical system components are monitored for successful replication across multiple data centers.	A1.3

IV Description of Criteria, Controls, Tests and Results of Tests

Relevant trust services criteria and BI Helper related controls are an integral part of management's system description and are included in this section. BI Helper performed testing to determine if its controls were suitably designed and operating effectively to achieve the specified criteria for the Security, Availability and Confidentiality categories set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy* (AICPA, *Trust Services Criteria)* through the period from 10/1/2023 to 3/31/2024.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of BI Helper activities and operations, and inspection of BI Helper documents and records. The results of those tests were considered in the nature and extent of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all BI Helper controls, this test was not listed individually for every control in the tables below.

Description of Company Controls	Criteria Number	Test of Controls	Result
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
The company establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet.	CC1.1.1	Inspected the company Code of Business Conduct made available to employees to determine the company establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet.	Policy attachment - Policy > CC1.1.
The company requires that new employees review and acknowledge the Code of Business Conduct upon hire, and that all staff members review and acknowledge it annually.	CC1.1.2	All employees acknowledge the Code of Business Conduct.	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
The company's Senior Management reviews and approves all company policies annually.	CC1.2.1	Policies are reviewed and updated annually.	Last policy update exercise on 4th Jan 2024.

The company's Senior Management reviews and approves the "Internal Audit Assessment" report annually.	CC1.2.2	Management reviews "Internal Audit Assessment" reports twice a year..	
The company's Senior Management reviews and approves the Organizational Chart for all employees annually.	CC1.2.3	Not relevant at current employee strength.	
The company's Senior Management reviews and approves the "Risk Assessment Report" annually.	CC1.2.4	Twice in a year, the report is reviewed.	
The company's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	CC1.2.5	Vendor Reports are reviewed annually.	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
The company maintains an Organizational Structure to define authorities, facilitate information flow and establish responsibilities.	CC1.3.1	At current employee strength, only Ishan and Kiran facilitate information flow and establish responsibilities. Only one other permanent employee and two consultants..	
The company maintains job descriptions for client serving, IT and engineering positions to increase the operational effectiveness of employees within the organization.	CC1.3.2	Yes. Internally we maintain job descriptions.	
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			

The company ensures that new hires go through a reference check as part of their onboarding process.	CC1.4.1	Yes. Currently all hires (employees and contractors) are through reference checks.	
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
The company has established a Security Awareness Training, and its contents are available for all staff on the company intranet.	CC1.5.1	As a part of onboarding, all hires (employees and contractors) go through a mandatory Security Awareness Training.	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
The company requires that new staff members complete Security Awareness Training upon hire, and that all staff members complete Security Awareness training annually.	CC1.5.2	As a part of onboarding, all hires (employees and contractors) go through a mandatory Security Awareness Training.	
The company requires that all staff members review and acknowledge company policies annually.	CC1.5.3	All employees go through and acknowledge company policies.	
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
The company's systems generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	CC2.1.1	Have monitoring alerts setup to generate information that is reviewed and evaluated to determine impacts to the functioning of internal controls.	
The company makes all policies and procedures available to all staff members via the company intranet.	CC2.1.2	Made available via the shared Google drive.	
The company displays the most current information about its services on its website, which is accessible to its customers.	CC2.1.3	Yes. The entire traffic and conversions happen via the company website. Cannot not keep it updated.	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
The company establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet.	CC2.2.1	Code made available to the employees	Evidence under the Policy folder.
The company requires that new staff members complete Security Awareness Training upon hire, and that all staff members complete Security Awareness training annually.	CC2.2.2	Yes. All staff members go through security training.	
The company requires that all staff members review and acknowledge company policies annually.	CC2.2.3	Not required at the current employee strength.	
The company makes all policies and procedures available to all staff members via the company intranet.	CC2.2.4	Yes. Via a shared Google Drive.	
The company has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the company in the event there are problems.	CC2.2.5	Yes. Policies shared via Google Drive..	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			

The company requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	CC2.2.6	Yes	
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
The company displays the most current information about its services on its website, which is accessible to its customers.	CC2.3.1	Yes	
The company has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the company in the event there are problems.	CC2.3.2	Yes. Multiple contact points available on the website and the app.	
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
The company has formally documented policies and procedures to govern risk management.	CC3.1.1	Yes. Policy attached.	Evidence under Policies folder.

Description of Company Controls	Criteria Number	Test of Controls	Result
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
The company performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements	CC3.1.2	Yes. The audit is done twice a year and reviewed.	

CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
The company performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements	CC3.2.1	Yes. Done twice a year.	
Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the platform. Risks are mapped to mitigating factors that address some or all of the risk.	CC3.2.2	Yes.	Policy assessing the risks is attached.
The company requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	CC3.2.3	Yes.	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
The company performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements and collecting and reviewing the SOC reports of its sub-service organizations on an annual basis.	CC3.2.4		

CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
The company considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	CC3.3.1	Yes.	Policy attached.
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
The company performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements	CC3.4.1	Inspected the risk assessment documentation to determine the company performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements.	No exceptions noted

Description of Company Controls	Criteria Number	Test of Controls	Result
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	CC3.4.2	Yes.	
The company performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements and collecting and reviewing the SOC reports of its sub-service organizations on an annual basis.	CC3.4.3	Yes.	

CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
The company's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing and reviewing the internal control environment.	CC4.1.1	Yes.	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
The company uses AWS Audit Manager, Snyk and other tools, for a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	CC4.1.2	Automated tools used for continuous monitoring of the systems.	In evidence folder, have attached a snapshot of all the automated tools for monitoring the system.
The company's Senior Management reviews and approves all company policies annually.	CC4.1.3	Yes.	No exceptions noted
The company's Senior Management reviews and approves the "Internal Audit Assessment" report annually.	CC4.1.4	Yes	
The company's Senior Management reviews and approves the Organizational Chart for all employees annually.	CC4.1.5	Yes	
The company's Senior Management reviews and approves the "Risk Assessment Report" annually.	CC4.1.6	Yes	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
The company's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	CC4.1.7	Yes.	
The company reviews and evaluates all subservice organizations periodically, to ensure commitments to the company's customers can be met.	CC4.1.8	Yes	
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
The company has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the company in the event there are problems.	CC4.2.1	In the Information Security Policy the section that describes how to report incidents to determine the company has provided information to employees, via the Information Security Policy, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the company in the event there are problems.	Evidence under the Policy folder.
The company uses AWS Audit Manager, AWS Security Hub, AWS Config Manager, Snyk, ECR Automated Scanning for continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	CC4.2.2	Company uses automated tools for monitorings	Evidence showcasing these tools has been attached.

Description of Company Controls	Criteria Number	Test of Controls	Result

CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
The company's Senior Management reviews and approves all company policies annually.	CC4.2.3	Yes	
The company's Senior Management reviews and approves the "Internal Audit Assessment" report annually.	CC4.2.4	Yes	
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
The company has developed a set of policies that establish expected behavior with regard to the Company’s control environment.	CC5.1.1	Yes.	Code of Business conduct policy attached.
The company's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	CC5.1.2		Attached the Organizational chart and the roles and responsibilities.

Description of Company Controls	Criteria Number	Test of Controls	Result
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
The company uses AWS Audit Manager, AWS Guard Duty, SNYK, ECR Docker Image Scanner for continuous monitoring of the system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	CC5.2.1	The mentioned automated tools are used.	Snapshots attached
The company's Senior Management reviews and approves all company policies annually.	CC5.2.2	Yes.	

The company's Senior Management reviews and approves the "Internal Audit Assessment" report annually.	CC5.2.3	Internal Audit Assessment is done twice a year.	
The company's Senior Management reviews and approves the Organizational Chart for all employees annually.	CC5.2.4	Not relevant at current scale. (3 full time employees + contractors)	
The company's Senior Management reviews and approves the "Risk Assessment Report" annually.	CC5.2.5	Yes	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
The company's Chief Executive Officer reviews and approves the list of people with access to the production console annually.	CC5.2.6	Yes. Only two people (Kiran and Ishan) have access to production.	
The company's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	CC5.2.7	Yes.	
The company reviews and evaluates all subservice organizations periodically, to ensure commitments to the company's customers can be met.	CC5.2.8	Yes	
The company has developed a set of policies that establish expected behavior with regard to the Company's control environment.	CC5.2.9	Yes	
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			

The company makes all policies and procedures available to all staff members via the company intranet.	CC5.3.1	Yes, via Google Drive.	No exceptions noted

Description of Company Controls	Criteria Number	Test of Controls	Result
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
The company requires that all staff members review and acknowledge company policies annually.	CC5.3.2	Yes. All new hires have to go through and acknowledge all the company policies.	
The company requires that new staff members review and acknowledge company policies as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them.	CC5.3.3	Yes	
The company has developed a set of policies that establish expected behavior with regard to the Company's control environment.	CC5.3.4	Yes	
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
The company has developed an access control policy and an accompanying process to register and authorize users prior to being issued system credentials and granted the ability to access the system.	CC6.1.1	Yes and alongside internal access control policy is used where relevant.	Policy attached.

Description of Company Controls	Criteria Number	Test of Controls	Result
The company maintains a matrix that outlines which system components should be accessible to staff members	CC6.1.2	Yes	Policy attached.

based on their role.			
The company's Senior Management or the Information Security Officer periodically reviews and approves the list of people with access to the company's system.	CC6.1.3	Yes. Access is reviewed once every quarter.	
The company's Senior Management or the Information Security Officer periodically reviews and approves the list of people with Administrative access to the company's system.	CC6.1.4	Yes. Admin access is reviewed once every quarter.	
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
The company has developed an access control policy and an accompanying process to register and authorize users prior to being issued system credentials and granted the ability to access the system.	CC6.2.1	Yes.	Policy attached.

Description of Company Controls	Criteria Number	Test of Controls	Result
The company maintains a matrix that outlines which system components should be accessible to staff members based on their role.	CC6.2.2	Yes. We maintain a role * access matrix. Not very relevant at the current employee strength.	
Staff access to the company's systems are made inaccessible in a timely manner as a part of the offboarding process.	CC6.2.3	Yes. We have a detailed offboarding process.	Process attached.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			

The company maintains a matrix that outlines which system components should be accessible to staff members based on their role.	CC6.3.1	Yes. Defined in the role*access matrix.	
Staff access to the company's systems are made inaccessible in a timely manner as a part of the offboarding process.	CC6.3.2	Yes.	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
The company ensures that access to the Infrastructure provider's environment (production console) is restricted to only those individuals who require such access to perform their job functions.	CC6.3.3	Yes. Current production access is only with Kiran and Ishan.	
The company ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	CC6.3.4	Yes. The production DB is only accessible to Kiran and Ishan.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
The company relies on an infrastructure provider for hosting the systems supporting its production environment. As a result, there is no physical access available to its staff members.	CC6.4.1	Carved out to subservice organization for physical access control	The Criterion is carved out and the responsibility of the subservice organization.

Description of Company Controls	Criteria Number	Test of Controls	Result

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
The company provides guidance on decommissioning of information assets that contain classified information in the Media Disposal Policy.	CC6.5.1	The Data Retention Policy and the Media Disposal Policy determine the guidance on decommissioning of information assets that contain classified information in the Media Disposal policy.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
The company requires that all staff members with access to the production console use multifactor authentication to access the console.	CC6.6.1	The production console configurations for user access control list that all staff members with access to the production console use multifactor authentication to access the console.	Evidence in AWS Foundational Security Best Practices. Report attached.
The company requires that all staff members with access to the Change Management System use multifactor authentication to access the system.	CC6.6.2	Yes. Bitbucket is MFA controlled.	
The company requires that all staff members with access to the Company Email Service use multifactor authentication to access the service.	CC6.6.3	Yes. MFA enabled for G Suite.	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
The company requires that all endpoints with access to production systems are protected by malware-protection software.	CC6.6.4	Yes. Antivirus is mandatory and is installed on all company assets.	Attached snapshot of the tool monitoring our internal assets.
The company requires that all company-owned endpoints be encrypted to protect them from unauthorized access.	CC6.6.5	Yes. All the devices are encrypted and encryption is on for all the employees.	

The company requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	CC6.6.6	Yes. We audit the systems once every quarter. We check the system for the following: 1.Antivirus 2. Disk Encryption 3. Updated Device OS 4. Screen lock	
The company requires that all company owned endpoints be configured to auto-screen-lock after 15 minutes of inactivity.	CC6.6.7	Inspected evidence of the auto-screen lock configuration to determine the company requires that all company owned endpoints be configured to auto-screen lock after 15 minutes of inactivity.	No exceptions noted
Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the company's cloud provider.	CC6.6.8	The security group and Web Application Firewall are in place. Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule is a default on the company's cloud provider.	Snapshots attached.

Description of Company Controls	Criteria Number	Test of Controls	Result
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
The company requires that all company-owned endpoints be encrypted to protect them from unauthorized access.	CC6.7.1	All company owned assets are encrypted.	
All production database[s] that store customer data are encrypted at rest.	CC6.7.2	The databases by themselves are not encrypted at rest but the customer data stored within them is encrypted.	Evidence - AWS Foundational Best Practices
User access to the company's application is secured using https (TLS algorithm) and industry standard encryption.	CC6.7.3	All unsecure connections (HTTP) are forced to secure/encrypted connections (HTTPS/TLS). User access to the company's application is secured using https (TLS algorithm) and industry standard encryption.	Evidence - AWS Foundational Best Practices

The company maintains a list of production infrastructure assets and segregates production assets from its staging/development assets.	CC6.7.4	Yes. The production systems are guarded using AWS Guard Duty.	Evidence - AWS Foundational Best Practices
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
The company requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	CC6.8.1	Yes. As a quarterly exercise all the company owned assets are audited.	

Description of Company Controls	Criteria Number	Test of Controls	Result
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the company's cloud provider.	CC6.8.2	Have a security group (firewall) configuration for every host. Every production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the company's cloud provider. Also a web firewall with restrictions is in place.	Snapshots added, list of firewall rules added.
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
The company identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	CC7.1.1	SNYK, ECR Docker scanner in place.	Snapshot added
The company tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.	CC7.1.2	SNYK, ECR Docker scanner in place.	Snapshot added.
The company's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	CC7.1.3	Yes. AWS Cloudwatch and Security Hub, Guarduty alerts in place.	Snapshot added.

Description of Company Controls	Criteria Number	Test of Controls	Result
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
The company identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	CC7.2.1	SNYK and ECR Image Scanner in place.	Snapshot added.
The company tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.	CC7.2.2	Yes.	Policy/Documentation added.
The company's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	CC7.2.3	Yes. Cloudwatch alerts, security alerts are in place.	Covered under AWS Foundational Security practices. Snapshot added.
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
The company uses AWS Audit Manager, AWS Security Hub, AWS ECR (docker scanning) as a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	CC7.3.1	Yes automated tools in place to monitor and review health of the information security program.	Snapshot of the individual tools added.

Description of Company Controls	Criteria Number	Test of Controls	Result
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
The company requires that all employee endpoints be audited once a quarter to ensure that the Operating System version is current or next most current.	CC7.3.2	Yes. All company systems are audited and are kept up to date.	

The company maintains a record of information security incidents.	CC7.3.3	Security incidents maintained in AWS Security Hub and AWS config.	Snapshot attached.
The company identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	CC7.3.4	Using SNYK for regular vulnerability scans.	Added a snapshot of SNYK and ECR Docker image scanner.
The company tracks all vulnerabilities, and resolves them as per the Vulnerability Management Policy.	CC7.3.5	Policy added. Vulnerability management done via Snyk and ECR Docker image scanning.	Snapshot added for Snyk and Docker Image scanner.
The company's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	CC7.3.7	IAWS Security Hub and AWS Cloud Alerts are configured for all the resources	AWS Foundational Security/ Best practices snapshot added.

Description of Company Controls	Criteria Number	Test of Controls	Result
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
The company uses AWS Audit Manager, AWS Security Hub, AWS ECR (docker scanning) , a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	CC7.4.1	Yes. Automated tools used.	Snapshot provided.
The company has established an Incident Management and Response Policy, which includes guidelines and procedures to be undertaken in response to information security incidents. This is available to all staff members via the company intranet.	CC7.4.2	Yes	Policy/Documentation attached.
The company maintains a record of information security incidents.	CC7.4.3	Yes. All tracked via AWS and BitBucket SNYK PRs	Snapshot provided as evidence.

CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
The company has documented Business Continuity and Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	CC7.5.1	Yes.	Policy attached.
The company has a documented Data Backup Policy, and makes it available for all staff on the company intranet.	CC7.5.2	Yes.	Policy/Documentation attached.

Description of Company Controls	Criteria Number	Test of Controls	Result
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
The company has a documented Change Management Policy, which is available to all Staff Members via the company intranet.	CC8.1.1	Yes.	Policy attached.
The company uses a change management system to track, review and log all changes to the application code.	CC8.1.2	Yes. We use JIRA and Trello	
The company maintains a list of infrastructure assets and segregates production assets from its staging/development assets.	CC8.1.3	Yes. Separate staging and production	
The company's change management system is configured to enforce peer reviews for all planned changes. For all code changes, the reviewer must be different from the author.	CC8.1.4	Yes. Code reviews are enforced and PR merging is not allowed unless reviewed and approved.	Image attached.

Description of Company Controls	Criteria Number	Test of Controls	Result
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
The company has a documented Risk Assessment and Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the company's service commitments and system requirements.	CC9.1.1	Yes.	Documentation/Policy attached.
The company performs a formal risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify threats that could impair systems' security commitments and requirements	CC9.1.2	Yes.	Documentation attached.
Each risk is assessed and given a score in relation to the likelihood of it occurring and potential impact on the security, availability and confidentiality of the platform. Risks are mapped to mitigating factors that address some or all of the risk.	CC9.1.3	Yes	Policy attached.

Description of Company Controls	Criteria Number	Test of Controls	Result
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			

The company has a documented Risk Assessment and Management Policy that describes the processes in place to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the company's service commitments and system requirements.	CC9.2.1	Yes. Have a policy	Policy attached
The company has a documented Vendor Management Policy that provides guidance to staff on performing risk assessment of third-party vendors.	CC9.2.2	Yes	Policy attached.
The company performs a formal vendor risk assessment exercise annually, as detailed out in the Risk Assessment and Management Policy, to identify vendors that are critical to the systems' security commitments and requirements and collecting and reviewing the SOC reports of its sub-service organizations on an annual basis.	CC9.2.3	Yes.	
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
The company's Production assets are continuously monitored to generate alerts and take immediate action where necessary.	A1.1.1	Yes.	AWS Security Hub and AWS Foundational Security practices score attached.

Description of Company Controls	Criteria Number	Test of Controls	Result
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			

The company has a documented Data Backup Policy, and makes it available for all staff on the company intranet.	A1.2.1	Yes	Evidence attached.
The company backs-up their production databases periodically.	A1.2.2	Yes. Every 24 hours	
The company's data backups are restored and tested annually.	A1.2.3	Yes.	Snapshots attached.
The company has documented Business Continuity and Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	A1.2.4	BC, DR Policies in place and tested	Policies added
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
The company has documented Business Continuity and Disaster Recovery Policies, that establish guidelines and procedures on continuing business operations in case of a disruption or a security incident.	A1.3.1	Business Continuity, Disaster recovery plan in place and is reviewed once a year.	Policies and documentation attached.

Description of Company Controls	Criteria Number	Test of Controls	Result
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
The company's data backups are restored and tested annually.	A1.3.2	Yes. Automated backups on.	AWS Security Hub/ Foundational Security Best practices snapshot added in the evidence folder.
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			

The company has a documented Confidentiality Policy, and makes it available for all staff on the company intranet.	C1.1.1	Yes	Policy attached.
The company requires that all new staff acknowledge the company's confidentiality policy as part of their onboarding.	C1.1.2	Yes.	Policy attached.
The company has a documented Data Classification Policy, and makes it available for all staff on the company intranet.	C1.1.3	Yes.	Data classification policy attached.
All production database[s] that store customer data are encrypted at rest.	C1.1.4	No. The production database itself is not encrypted. However the customer data is encrypted and stored in the DB.	Attached a snapshot from AWS.

Description of Company Controls	Criteria Number	Test of Controls	Result
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
The company requires that all company-owned endpoints be encrypted to protect them from unauthorized access.	C1.1.5	Yes.	Attached a screenshot of monitoring of assets.
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
The company has a documented Data Retention Policy, and makes it available for all staff on the company intranet.	C1.2.1	Yes. Data retention policy is mentioned in EULA and communicated to the users.	EULA
The company provides guidance on decommissioning of information assets that contain classified information in the Media Disposal Policy.	C1.2.2	Yes.	Media disposal policy attached.

- **End of document** -