Visionify Inc.

(Visionify)

SOC 2 TYPE II REPORT

For The Period,

15th January 2024 to 15th July 2024

Independent Service Auditors' Report on Management's Description of a Service Organization's System Relevant to Security, Confidentiality and Availability and the Suitability of the Design and Operating Effectiveness of Controls

Prepared by:

[VISIONIFY]®

Table of Contents

SECTION 1

Independent Service Auditor’s Report

For the period, 15th January 2024 to 15th July 2024

Independent Service Auditor’s Report

To: Management of Visionify Inc. (Visionify)

Scope

We have examined the attached Visionify Inc. (Visionify) description of the system titled “Workplace Safety & Compliance Monitoring through existing CCTV cameras” **(**description) throughout the period 15th January 2024 to 15th July 2024 included in Section 3, based on the criteria set forth in the Description Criteria DC Section 200 *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2 Report* (description criteria) and the suitability of the design and operating effectiveness of controls included in the description throughout the period 15th January 2024 to 15th July 2024 to provide reasonable assurance that Visionify service commitments and system requirements would be achieved based on the trust service criteria for Security, Confidentiality and Availability set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for *Security, Availability, Processing Integrity, Confidentiality and Privacy* (applicable trust services criteria).

The information included in Section 5, “Other Information Provided by Visionify ” is presented by management of Visionify to provide additional information and is not a part of Visionify description of its system made available to user entities during the period 15th January 2024 to 15th July 2024. Information about Visionify business continuity planning etc. has not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the system.

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Visionify controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

As indicated in the description, Visionify uses subservice organization Azure for data center services. The description in Section 3 includes only the controls of Visionify and excludes controls of the various subservice organizations. The description also indicates that certain trust services criteria can be met only if the subservice organization’s controls, contemplated in the design of Visionify controls, are suitably designed and operating effectively along with related controls at the service organization. Our examination did not extend to controls of various subservice organizations for data center services.

Service Organization's Responsibilities

Visionify is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the service commitments and system requirements were achieved.

Visionify has provided the accompanying assertion titled, Management of Visionify Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirement would be achieved based on the applicable trust services criteria if operating effectively. Visionify is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the applicable trust services criteria stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the presentation of the description based on the description criteria set forth in Visionify assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is presented in accordance with the description criteria and (2) the controls are suitably designed and operating effectively to meet the applicable trust services criteria stated in the description throughout the period 15th January 2024 to 15th July 2024.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is fairly presented and that the controls were suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs. Because of their nature, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, conclusions about the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria are subject to the risks that the system may change or that controls at a service organization may become ineffective.

Opinion

In our opinion, in all material respects, based on the description criteria described in Visionify assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented throughout the period 15th January 2024 to 15th July 2024>.

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period 15th January 2024 to 15th July 2024>, and the subservice organization and user entities applied the controls contemplated in the design of Visionify controls throughout the period 15th January 2024 to 15th July 2024>.

c. The controls operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period 15th January 2024 to 15th July 2024, and user entities and subservice organization applied the controls contemplated in the design of Visionify controls, and those controls operated effectively throughout the period 15th January 2024 to 15th July 2024>.

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of our tests are presented in the section 4 of our report titled "Independent Service Auditors' Description of Test of Controls and Results".

Restricted Use

This report, including the description of controls and results thereof in Section 4 of this report, is intended solely for the information, and use of Visionify; user entities of Visionify systems during some or all of the period 15th January 2024 to 15th July 2024; and those prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization’s system interacts with user entities, subservice organizations or other parties
- Internal control and its limitations
- User entity responsibilities, Complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

For,

Accorp Partners CPA LLC

Digitally signed by Accorp Partners CPA LLC
Date: 2024.08.13 00:43:50 -07'00'

Accorp Partners CPA LLC
License no: PAC-FIRM-LIC-47383
Date: August 13, 2024

SECTION 2

Management Assertion

July 31, 2024

Management of Visionify Inc. Assertion

We have prepared the accompanying description of **Visionify Inc.** (Visionify). system titled **Workplace Safety & Compliance Monitoring through existing CCTV cameras** throughout the period 15th January 2024 to 15th July 2024 (description), based on the criteria set forth in the Description Criteria DC Section 200 2018 Description Criteria for a Description of a Service Organisation's System in a SOC 2 Report (description criteria).

The description is intended to provide users with information about **Workplace Safety & Compliance Monitoring through existing CCTV cameras** that may be useful when assessing the risks arising from interactions with **Visionify Inc.** system, particularly information about the suitability of design of **Visionify Inc.**'s controls to meet the criteria related to Security, Availability and Confidentiality set forth in TSP Section 100, 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.

Visionify Inc. uses Azure that provides data center services. The description includes only the controls of **Visionify Inc.** and excludes controls of the subservice organizations. The description also indicates that certain trust services criteria specified therein can be met only if the subservice organization controls contemplated in the design of **Visionify Inc.** controls are suitably designed and operating effectively along with related controls at the service organization. The description does not extend to controls of the subservice organizations.

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of **Visionify Inc.'s** controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of user entities.

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

a. the description fairly presents the **Workplace Safety & Compliance Monitoring through existing CCTV cameras** throughout the period 15th January 2024 to 15th July 2024 based on the following description criteria:

i. The description contains the following information:

1) The types of services provided
2) The components of the system used to provide the services, which are as follows:
   a) Infrastructure. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and other telecommunications networks).
   b) Software. The application programs and IT system software that support application programs (operating systems, middleware, and utilities).
   c) People. The personnel involved in the governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
   d) Procedures. The automated and manual procedures.
   e) Data. Transaction streams, files, databases, tables, and output used or processed by the system.
3) The boundaries or aspects of the system covered by the description.
4) For information provided to, or received from, subservice organizations or other parties,
   a) how such information is provided or received and the role of the subservice organization and other parties and

   b) the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

5) The applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, the following:
   a) Complementary user entity controls contemplated in the design of the service organization's system.
   b) When the inclusive method is used to present a subservice organization, controls at the subservice organization
6) If the service organization presents the subservice organization using the carve out method,
   a) the nature of the services provided by the subservice organization and
   b) each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria.
7) Any applicable trust services criteria that are not addressed by a control at the service organization or a subservice organization and the reasons.

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in the description were suitably designed throughout the period 15th January 2024 to 15th July 2024 to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated as described and if user entities applied the complementary user entity controls, and the subservice organization applied the controls contemplated in the design of **Visionify Inc.** controls.

Sincerely,

H.A.Murari

Harsh Murari
CTO, Visionify Inc.
Email: hmurari@visionify.ai
Phone: 303-408-9848

SECTION 3

Description Of Visionify Inc. Services and Products

From 15th January 2024 to 15th July 2024

Background and Overview of Services

Visionify is computer Vision company based in Denver, CO, focused on delivering innovative solutions for Workplace Safety and Compliance.

Services provided by Visionify Inc. includes below:

Line of Products –

VisionAI

At Visionify, we are dedicated to revolutionizing Environmental, Health, and Safety standards through our powerful Vision AI applications. Our Vision AI suite offers a comprehensive suite of workplace safety and compliance solutions that are designed to detect potential hazards, monitor worker safety and prevent accidents. Available on Azure Marketplace, these Ready-to-use, pre-trained apps can be accessed easily through CLI and web-based GUI.

Significant Changes during the Review Period

None

Subservice Organizations

Visionify Inc. utilizes the following subservice providers for data centre services that are not included within the scope of this examination. However, Visionify Inc. responsibilities for the applications and services run at these cloud services are covered as part of the audit and in scope. Responsibility matrix is defined as part of the SLA and agreements with these sub-service organizations.

Microsoft Azure (Azure)

Azure has provided an Independent Service Auditor's Report (SOC2).

The Criteria that relate to controls at the subservice organizations included all criteria related to the Trust Service Principles of Security, Confidentiality and Availability. The types of controls that are necessary to meet the applicable trust services criteria, either alone or in combination with controls at Visionify Inc. include:

- The system is protected against unauthorized access (both physical and logical).
- The system is available for operation and use and in the capacities as committed or agreed.
- Policies and procedures exist related to security and availability and are implemented and followed.

Principal Service Commitments and System Requirements

Visionify Inc. designs its processes and procedures related to the System to meet its objectives. Those objectives are based on the service commitments, related laws and regulations of products and services, financial, operational, and other compliance requirements that has established for such services. Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online.

Visionify Inc. establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Visionify Inc. 's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach as to how the systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

Components of the System

The System is comprised of the following components:

- Infrastructure including the physical structures, Information Technology (IT) and other hardware.
- Software including application programs and IT system software that support application programs.
- People including executives, sales and marketing, client services, product support, information processing, software development, IT, Finance and Human resources.
- Procedures (automated and manual).
- Data including transaction streams, files, databases, tables, and output used or processed by the system.

The System boundaries include the applications, databases and infrastructure required to directly support the services provided to Visionify Inc.'s clients. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to Visionify Inc.'s customers are not included within the boundaries of its system.

Boundaries of the System

The specific products, services and locations that are included in the scope of the report are given below. All other products, services and locations are not included.

Products and Services in Scope
Products ● VisionAI
Geographic Locations in Scope
1499 W 120th Ave #110, Westminster, CO 80234, United States

All the above material activities and operations in scope are performed from the above office location. Unless otherwise mentioned, the description and related controls apply only to the location covered by the report.

Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information and Communication

Control Environment

Visionify Inc.'s internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls, and the emphasis given to controls in the Company's policies, procedures, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management is committed to the Information Security Management System, and ensures that IT Security policies are communicated, understood, implemented, and adhered at all levels of the organization and regularly reviewed for continual suitability.

Integrity and Ethical Values

Visionify Inc. requires directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the Company, and all employees are expected to fulfil their responsibilities based on these principles and comply with all applicable laws and regulations. Visionify Inc. promotes an environment of open communication and has created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

Board of Directors

Business activities at Visionify Inc. are under the direction of the Board of Directors. The company is governed by its Board of Directors headed by its founder Priyesh Sanghvi. Priyesh Sanghvi is in charge of the company's Global operations playing a key role in strategy and client management.

Management's Philosophy and Operating Style

The Executive Management team assesses risks prior to venturing into business ventures and relationships. The Executive Management team to interact with operating management on a daily basis.

Risk Management and Risk Assessment

Risk assessments are performed annually to identify current risk levels, with recommendations to minimize those risks that are determined to pose an unacceptable level of risk to Visionify Inc.. As part of this process, security threats are identified and the risk from these threats is formally assessed.

Visionify Inc. has operationalized a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User Organizations. This process consists of Information Security team identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks.

Following steps are involved in performing risk assessments

- Risk identification for each asset in a process and at Organizational level.
- Risk analysis & evaluation for each asset in a process & at Organizational level.
- Risk treatment & residual risk.

Risk assessment comprises of calculating the level of risk associated with assets belonging to a particular business process. It is done in a manner to assess and evaluate the criticality of impact on business by a particular risk also to identify the areas where organization needs to focus over information security. Apart from the asset-based risk assessment, the Company has also conducted organization-based risk assessment which is based on internal as well as external issues, needs and expectations of interested parties etc. The threats, vulnerabilities associated with every asset are evaluated along with threat impact, probability of occurrence and chances of detection (on a rating basis) of the threat. This determines the Risk Factor, which is then put into an equation to derive a risk value. The risk value is then compared to the organizational threshold (i.e., accepted risk value) which is treated appropriately (i.e., treat, transfer, avoid, accept). The identified risks will be treated (mitigated) so that risk levels are reduced. The output of a risk assessment will include a complete risk register and risk treatment plan. Any action plans are tracked to completion. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

Information Security Policies

Visionify Inc. has developed an organization-wide Information Security Policies. All the people impacting Security Policies (IS Policies) are made available to employees via Scrut Portal. Changes to the Information Security Policies are reviewed by IS Team and approved by CEO/CTO prior to implementation.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in business conditions. Management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities. Performance monitoring reports cover server parameters such as disc space, incoming/outgoing network traffic, packet loss, CPU utilization etc. These system performance reports are reviewed by management on a periodic basis. In addition, a self-assessment scan of vulnerabilities is performed prior every release to the production or on yearly basis. Vulnerabilities are evaluated and remediation actions monitored and completed. Results and recommendations for improvement are reported to management.

Information and Communication

Visionify Inc. has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based upon suggestions from security personnel and approval by management. Departmental managers monitor adherence to policies and procedures as part of their daily activities. The management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. CTO the focal point for communication regarding the IT environment. Additionally, there are personnel that have been designated to interface with the customer if processing or systems development issues affect customer organizations. Electronic messaging has been incorporated into many of Visionify Inc.'s processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with employees.

Electronic Mail (e-Mail)

Communication to Customer organizations and project teams are done through e-mail. Important corporate events, employee news, and cultural updates are some of the messages communicated using e-mail. E-mail is also a means to draw the attention of employees towards adherence to specific procedural requirements. Visionify Inc. requires two factor authentications from employees to access their e-mails.

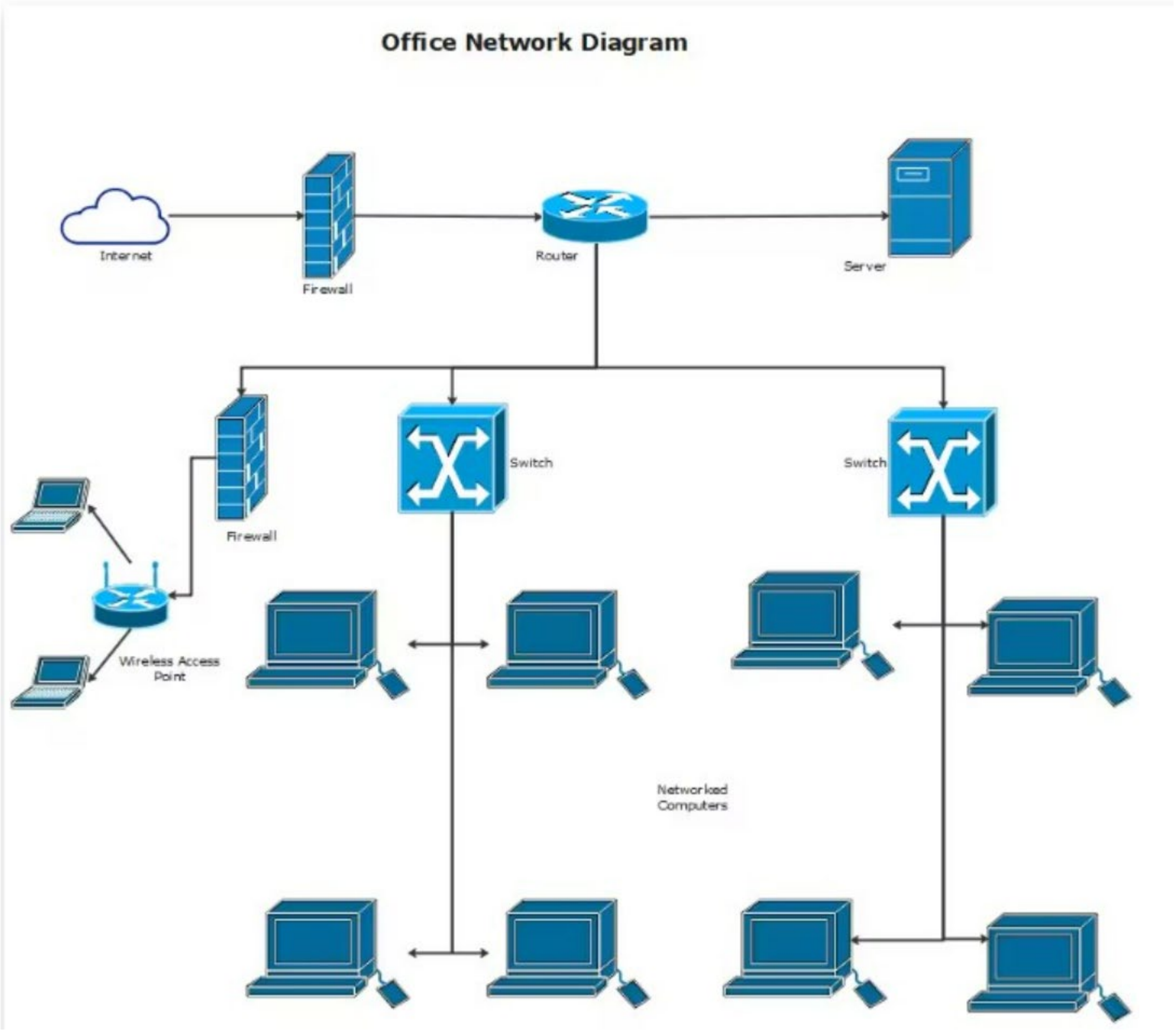
Components of the System

Infrastructure

The infrastructure comprises physical and hardware components of the System including facilities, equipment, and networks.

Network Segmentation Overview

Visionify Inc.'s offices are equipped with the latest hardware, software, and networking infrastructure. All the offices are linked through high-speed communication channels, backed up by redundant networks.



Software

Firewalls

The production system at Azure is protected by security group rules (virtual firewall) set up for the virtual private cloud (VPC) provided by Azure. VPC is used to protect all Production systems hosted at Azure. Any change to configuration is overseen by the IT Security team. All configuration, backup and rules have been documented for compliance.

Network & Endpoint protection

All systems and devices are protected by the comprehensive endpoint protection system. The endpoints include antivirus, anti-malware, and Trojan protection from any source. This also includes the e-mail scanning of the systems which prevents malicious scripts and viruses from the e-mails. Apart from which all systems are restricted to internet with the content filtering system routed through the proxy server.

Monitoring

Visionify Inc. has implemented adequate monitoring controls to detect unauthorized information processing activities. Critical servers and systems are configured to log user activities, Exceptions, and information security events. System Administrator activities are logged and reviewed on a periodic basis.

Capacity Management

Capacity management controls are put in place so as to monitor, tune and project certain Visionify Inc.'s resources to ensure system performance meets the expected service levels and minimize the risk of systems failure and capacity related issues. Addition of new information systems and facilities, upgrades, new version and changes are subject to formal system analysis, testing, and approval prior to acceptance.

Patch Management

The respective vertical team of Windows/Network team ensures that all patches to network device/servers operating systems are tested for stability & availability issues before deploying to the production environment. The patch management activity is done regularly or as and when any critical event occurs and required updates or patch are installed to ensure efficient working of the servers, desktops, and critical network devices. Operating system patches related and marked critical, and security are managed and applied as they become available, windows systems are managed through the patch management system and the network devices OS patching is managed automatically while renewing.

Vulnerability Scans & Security Audits

As per the Audit calendar, all the network devices and services are audited for vulnerabilities by doing periodic vulnerability scans. These scans are done by internal IT Infrastructure team.

Virus Scans and Endpoint Security

Windows Defender is installed with the feature of scanning the device automatically and log reports are reviewed by the IT Head. Anti-virus software has been installed on all desktops & laptops within the scope. Updates to the virus definition files are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals.

People

Organizational Structure

The organizational structure provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups according to their job responsibilities. This approach helps to enable the organization to define responsibilities, lines of reporting, and communication, and helps facilitate employees to focus on the specific business issues impacting clients.

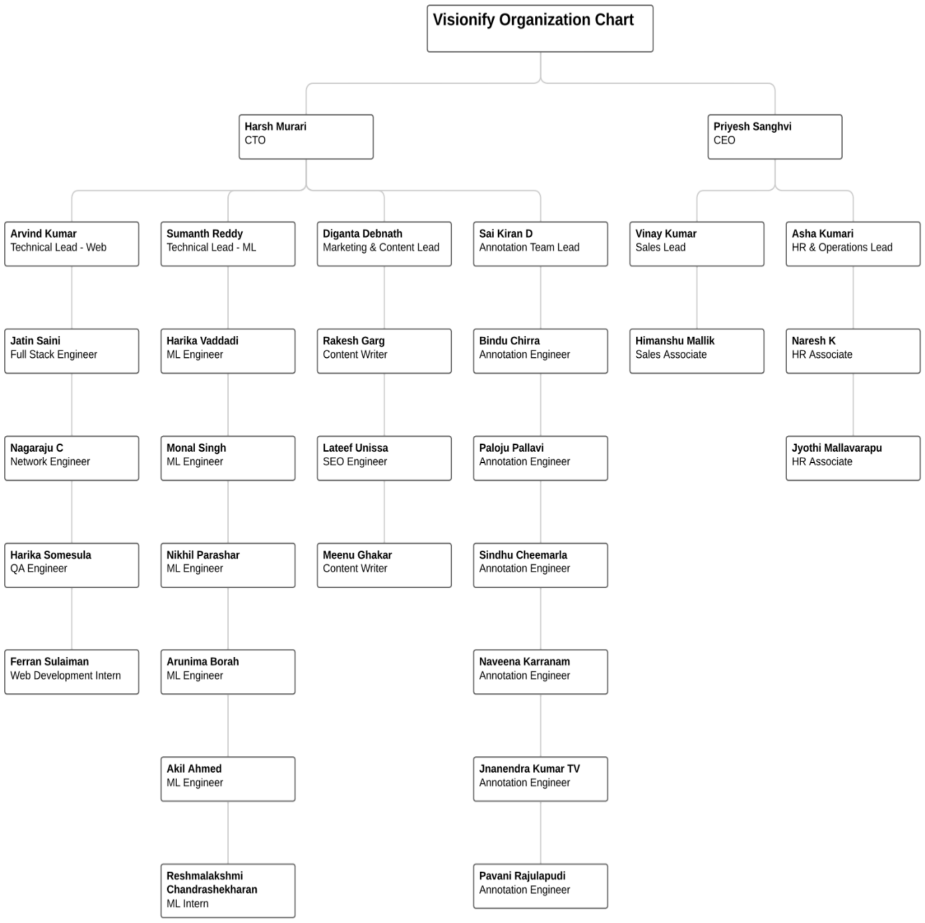
The management team meets regularly to review business unit plans and performances. Meetings with the CEO and department heads are held to review operational, security and business issues, and plans for the future.

Visionify Inc.'s Information Security policies define and assign responsibility/accountabilities for information security. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

Roles and Responsibilities

The following are the responsibilities of key roles.

IT Security Organisation Chart



Roles and Responsibilities

The following are the responsibilities of key roles.

Chief Executive Officer (CEO)

- The CEO’s responsibilities, with respect to IT security, are as follows:
- Ensure that appropriate levels of security are applied to all IT assets.
- Ensure that Visionify Inc. ’s has established IT security program.
- Allocate sufficient resources necessary for the protection of Visionify Inc. ’s IT assets;
- Hold Visionify Inc. ’s managers accountable for the security of the IT assets under their control.

- Ensure that staff, facilities, and IT processing assets with appropriate national security clearances are available in the Office of the Director, Visionify Inc. .

Chief Technology Officer (CTO)

The CTO's responsibilities, with respect to IT Security, the CTO's responsibilities are as follows:

- Ensure that appropriate levels of security are applied to all IT assets (whether retained in-house or under the control of contractors); and
- Oversee, define, plan, budget, and implement the IT security program; and
- Approve and issue IT security program policy, procedures, and guidance; and
- Ensure that the IT security program integrates fully into enterprise architecture and capital planning and investment control processes.
- Ensure that IT assets are developed and operated in full compliance with Department and Visionify Inc. 's policies, as well as ISO 27001's IT security-related directives.
- Ensure that all IT assets owned or operated by or for Visionify Inc. 's are accredited
- Ensure that IT security is planned and implemented across Visionify Inc. 's throughout all phases of the System Development Life Cycle.
- Provide an IT processing procedures manual for classified information to all cleared staff; and
- Provide an IT processing procedures manual to all staff that includes processing procedures for information commonly considered “sensitive information”.

Chief Information Security Officer (CISO)

CISO responsibilities are as following:

- Coordinate implementation of the IT security program.
- Develop IT security program policy, procedures, standards, and guidance consistent with Departmental and ISO 27001's requirements.
- Assist with the development of IT system specific policy, procedures, and safeguards.
- Implement and manage an IT security awareness and training program.
- Assist with the planning and budgeting of IT security functions for Visionify Inc. .
- Establish and maintain an IT security certification and accreditation program. This includes ensuring that all assets have completed and maintained security plans, risk assessments, contingency plans, and security self-assessments.
- Ensure that an objective, independent review, and approval process exists for both security plans and procurement requests to validate the adequacy of proposed security safeguards.
- Communicate security requirements to Visionify Inc. 's management and staff and serve as a resource on effective IT security practices.
- Act as a liaison between the Department and Visionify Inc.'s on Department-wide security initiatives, incident response activities, and on fulfilling IT security reporting requirements.
- Conduct Visionify Inc.-wide intrusion detection and vulnerability monitoring; and
- Create and maintain an incident response capability.

IT Manager

IT Manager's Various security responsibilities are:

- Coordinate Serve as a co-accreditor of all IT assets. Operating Unit Directors are the designated approving authority (accepting operating risk) for the operating unit's IT assets, but the CIO must co-accredit all IT assets.
- Ensure that all cleared staff receive an extensive briefing presented by a qualified staff member relevant to their clearance level that describes in detail all individual IT responsibilities prior to granting access to any classified assets.
- Ensure that all cleared staff receive a comprehensive yearly awareness briefing presented by a qualified staff member of individual IT responsibilities relevant to their clearance level as a condition of continued access to any classified assets.

Department Heads

Department Heads are directly responsible for the security of the assets under their purview. Department Heads have the following responsibilities:

- Ensure that appropriate levels of security are applied to all the assets and that sufficient resources are planned and assigned to maintain the required level of security.
- Work closely with and support the CISO in implementing the Visionify Inc.'s IT security program.
- Ensure all assets are developed and operated in full compliance with Department and policies (e.g., annual user training requirements) as well as ISO 27001's IT security-related directives and mandates.
- Account for IT security in capital investment plans which must include all IT resources (e.g., labor, hardware, software, maintenance) for procurement, maintenance, and replacement of all assets.
- Ensure IT security is planned and implemented throughout all phases of the System Development Life Cycle.
- Ensure that department positions with significant security responsibilities are held by staff with sufficient training and education qualifications as well as by staff who have had appropriate background checks.
- Designate alternate ISO(s) for when the primary ISO(s) is unavailable.
- Assign ownership of IT resources such that all department resources are assigned to a particular system and such that all assets have a designated system owner.
- Serve as the Designated Approving Authority (accepting operating risk) for the department's assets along with the CTO who co-accredits all IT assets.
- Ensure that staff responsible for oversight of Visionify Inc.'s classified information processing efforts receive extensive training from the agencies that sponsor those efforts, including yearly refresher briefings presented by those agencies.
- Ensure that all cleared staff receive an extensive briefing presented by a qualified staff member relevant to their clearance level that describes in detail all individual IT responsibilities prior to granting access to any classified assets; and
- Ensure that all cleared staff receives a comprehensive yearly awareness briefing presented by a qualified staff member of individual IT responsibilities relevant to their clearance level as a condition of continued access to any classified assets.

System owners and data owners

- System and Data owners are employees with managerial, operational, technical, and often budget responsibility for all aspects of an IT system Specifically, they have the following responsibilities:
- Ensure that appropriate levels of security are applied to the IT system and that sufficient resources are planned and assigned to maintain this level of security.
- Ensure the system is developed and operated in full compliance with Department and Visionify Inc.'s policies as well as ISO 27001's IT security-related directives and mandates.
- Determine the system sensitivity levels (high, medium, or low) with respect to confidentiality, integrity, and availability concerns.
- Ensure IT security is planned and implemented throughout all phases of the System Development Life Cycle.
- Ensure that appropriate security requirements and disclosure agreements are included in the specifications for the acquisition of IT and IT services and certify that awarded contracts comply with security requirements.
- Ensure that the IT system is meeting all applicable certification and accreditation requirements.
- Ensure that security breaches are reported in accordance with Visionify Inc.'s policy and procedure.
- Ensure that IT system users receive appropriate security training.
- Determine the appropriate position sensitivity designations for critical and sensitive employee positions (e.g., system administrators) and ensure that staff and associates under their jurisdiction have undergone appropriate background investigations. Inform staff and associates of the level of security that must be maintained given their position sensitivity.
- Ensure system specific security responsibilities are properly identified and documented. Ensure that duties are separated among multiple employees whenever necessary to prevent a single person from performing malicious or illegal activities undetected.
- Ensure that system positions with significant security responsibilities are held by staff with sufficient training and education qualifications as well as by staff who have had appropriate background checks.

All Administrators

All administrators (database, application, system, and network administrators) are those who maintain database, application, system, and network. Each administrator is responsible for the secure operation and maintenance of the IT elements under their control. Specifically, administrators have the following responsibilities:

- Ensure that IT system technical and operational security controls are being implemented and maintained according to the sensitivity level of the system and the data being processed.

- Assist in the development and maintenance of required security documentation and related activities (e.g., system administration and operational procedures and manuals).
- Know which assets or parts of assets for which they are directly responsible.
- And assist the ISO, the system owner, and the department IT Security Officer as necessary.
- Coordinate with appropriate system administrators and ISOs to ensure that their databases and applications are being adequately protected commensurate with the sensitivity level of the data being processed.
- Operate databases and applications in a secure manner.
- Manage user accounts in a timely and secure manner (e.g., disabling accounts).
- Assist in the development and maintenance of required security documentation and related activities (e.g., application administration and operational procedures and manuals).
- Know which applications and databases for which they are directly responsible.
- And assist the ISO and the department IT Security Officer, as necessary.

Assignment of Authority and Responsibility

Management is responsible for the assignment of responsibility and delegation of authority within Visionify Inc. .

Human Resources Policies and Procedures

Visionify Inc. maintains written Human Resources Policies and Procedures. The policies and procedures describe practices relating to hiring, training and development, performance appraisal and advancement and the termination. Human Resource ('HR') policies and practices are intended to inform employees on topics such as expected levels of integrity, ethical behaviour, and competence.

The Human Resources department review these policies and procedures on periodic basis to ensure they are updated to reflect changes in the organization and the operating environment. Employees are informed of these policies and procedures upon their hiring during Induction. Personnel policies and procedures are documented in the Human Resources Policy.

New Hire Procedures

New employees are required to read and accept HR corporate policies and procedures and are provided online access to these policies. Hiring procedures require that the proper educational levels have been attained along with required job-related certifications, if applicable, and industry experience. If a candidate is qualified, interviews are conducted with various levels of management and staff.

Reference checks are completed for prospective employees. Employees are required to sign Employee Confidentiality Agreement which forms an integral part of employee file. Discrepancies Noted in background investigations are documented and investigated by the Human Resources Department. Any discrepancies found in background investigations result in disciplinary actions, up to and including employee termination.

New Joiner Trainings

HR coordinates to provide HR training and information security awareness program to all employees as part of induction. HR maintains the records of information security awareness training namely onboarding tracker and feedback forms from employees.

Employees are required to complete security awareness training at the time of joining. Training is documented, monitored, and tracked by management.

Employee Terminations

Termination or change in employment is processed as per extant HR related procedures. There are clearly identified and assigned responsibilities with regard to termination or change in employment. All employees, contractors and third-party personnel are required to return physical and digital Identification/access tokens provided to them by or its clients on their termination of employment or contract.

Access privileges are revoked upon termination of employment, contract, or agreement. In case of change of employment/role, rights associated with prior roles are removed and new access privileges are created as appropriate for the current job roles and responsibilities.

Code of Conduct and Disciplinary Action

Visionify Inc. has put forward Code of Conduct and Disciplinary Process in-order to encourage and maintain standards of conduct and ensure consistent and fair treatment for all. An employee whose conduct does not comply with an element of the code of conduct and has been found to have breached the same is prosecuted as per defined process and policies.

Procedures

IT policies and operating instructions are documented. Procedures described cover server management, server hardening, workstation security system, network management, security patch management, user creation, system audit, ID card activation, etc. Additionally, production and training standard operating procedures are available.

Help Desk

Visionify Inc. has put in place an IT helpdesk function to handle problems and support requirements of users, support users in case of incidents and manage them without disruption to business and ensures that changes to any component of Visionify Inc.'s information assets and infrastructure are controlled and managed in a structured manner. All requests are logged thru helpdesk and resolved within the maximum resolution time as defined.

Change Management

Visionify Inc. has implemented a well-defined Change management process to ensure that all changes to the information processing facilities, including equipment, supporting facilities and utilities, networks, application software, systems software and security devices are managed and controlled. The Change Management process describes a methodical approach to handle the changes that are to be made. All the changes need to be subjected to a formal Change Management process.

Every change to such base lined components is governed by the change control and management procedures as outlined in the Helpdesk, Change management and Incident Response procedure. Visionify Inc.'s change management process requires all security patches and system and software configuration changes to be tested before deployment into Stage or Production environments.

All changes are recorded, approved, implemented, tested and versioned before moving to production environment. The impact of implementing all significant changes are analysed and approved by the IS team Head before such implementation. A sign-off obtained from the personnel who had requested for the change after implementation of the change.

Incident Response and Management

Procedures for the incident response including identification and escalation of security breaches and other incidents are included in the policy. Users or any other person log all incidents to the Helpdesk. For Network incidents, IT team received incident tickets via email and are resolved by them.

The help desk personnel or IT team study and escalate all security incidents to the designated team for further escalation/resolution. All security incidents are reviewed and monitored by the IT Team. Corrective and preventive actions are completed for incidents.

When an incident is detected or reported, a defined incident response process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures and the actions proposed are approved by CTO.

Logical Access

Security Authorization and Administration

Email is sent from HR to IT helpdesk for all new employees for a new workstation configured with minimum default access to company resources/applications required by an employee to perform the job duty. The default access levels for different departments are defined and documented in HR/Admin policy and IS policies. Any additional access is recommended by the line manager and approved IT Head. Company has standard configuration that is implemented across Desktops & laptops individually.

Access to resources is granted to an authenticated user based on the user's identity through a unique login ID that is authenticated by an associated password. Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles.

Roles are periodically reviewed and updated by asset owners regularly. Privileged access to sensitive resources is restricted to IT team and authorized users of the DevOps team. Access to storage, backup data, systems, and media is limited to IT team through the use of physical and logical access controls.

Security Configuration

Employees establish their identity to the local network and remote systems through the use of a valid unique user ID that is authenticated with the associated password. Remote access to critical resources is not permitted to any employee. Passwords are controlled through Password policy of the domain controller and include periodic forced changes, password expiry and complexity requirements. User accounts are disabled after a limited number of unsuccessful logon attempts; the user is required to contact the IT Support team to reset the password. Local users do not have access to modify password rules. Guest and anonymous logins are not allowed on any machines. Unattended desktops are locked within a time of inactivity. Users are required to provide their password to unlock the desktop.

Administrative Level Access

Administrative rights and access to administrative accounts are granted to individuals that require that level of access in order to perform their jobs. All administrative level access, other than to IT team, must be justified to and approved by IT team.

Confidentiality

Secure procedures are established to ensure safe and secure disposal of media when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the information classification guideline.

Backup and Recovery of Data

Visionify Inc. has developed formal policies and procedures relating to backup and recovery. Backup is defined in the Backup Policy. Suitable backups are taken and maintained. The backup processes are approved by the business owners and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods as defined in the "Backup Policy".

Applicable Trust Services Criteria and related Controls

The Security, Confidentiality and Availability trust services categories and Visionify Inc. related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results".

Visionify Inc. has determined that Processing Integrity & Privacy trust services Categories are not relevant to the system.

User- Entity Control Considerations

Services provided by Visionify Inc. to user entities and the controls of Visionify Inc. cover only a portion of the overall controls of each user entity. Visionify Inc. controls were designed with the assumption that certain controls would be implemented by user entities. In certain situations, the application of specific controls at user entities is necessary to achieve relating to the services outlined in this report to be achieved solely by Visionify Inc.. This section highlights those internal control responsibilities that Visionify Inc. believes should be present for each user entity and has considered in developing the controls described in the report. This list does not purport to be and should not be considered a complete listing of the controls relevant at user entities. Other controls may be required at user entities.

- User Organizations are responsible for ensuring that complete, accurate and timely information is provided to Visionify Inc. for processing.
- User Organizations are ultimately responsible to limit access to only those Visionify Inc. employees who are required to perform their job responsibilities and that all users are assigned unique accounts.
- User Organizations are responsible for monitoring and reviewing their business processes.
- User Organizations are responsible for ensuring end customer privacy.

- User Entity should establish confidentiality procedures to ensure that all inputs have been authorized, have been accepted for processing, and are accounted for. Any missing or unaccounted source documents or input files have been identified and investigated. These processes require that exceptions be resolved within a specified time period.
- User Organizations are responsible for defining criteria for processing and rejecting items input into their systems.
- User Organizations are responsible for working with Visionify Inc. to resolve any input discrepancies or quality issues.
- User Organizations are responsible for reviewing the completeness and accuracy of the inputs / processing services performed by Visionify Inc..
- User Organizations are responsible for working with Visionify Inc. to jointly establish service levels and revise the same based on changes in business conditions.
- User Organizations are responsible for initiating and implementing changes to the applications managed by User Organizations.

SECTION 4

Trust Services Security, Confidentiality and Availability

Principles Criteria & Related Controls

Trust Services Security, Confidentiality and Availability, Criteria & Related Controls and Test of effectiveness and Results of Test

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	Control environment		
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**		
	The Company has a mission and vision statements. Additionally, the entity has developed a clearly articulated statement of ethical values that is understood at all levels of the organization. The communication Mission, Vision and Ethical statement is through shared drive screenshot.	Inspected Induction PPT to determine that mission and vision statements of ethical values are established.	No Exceptions Noted
	The Company has approved code of conduct that is applied across the entity. Code of Conduct policy is posted on the shared directory and GRC Platform. The Code of Conduct outlines strict disciplinary consequences for violation of code of conduct	Inspected Code of Conduct on shared directory and GRC Platform to determine that Code of Conduct outlines strict disciplinary consequences for violation of code of conduct.	No Exceptions Noted
	All new employees are provided training and are made to sign code of conduct. New employees sign off that they have read this document. Existing employees, on an annual basis, undergo refresher training on Company's policies on code of conduct. COC posted on the shared directory	Inspected Induction training deck to determine that CoC training is given to all employees at least once a year.	No Exceptions Noted
	Performance appraisals are performed at least annually.	Inspected HR Process Handbook to determine that Performance appraisals are performed at least annually.	No Exceptions Noted
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed by appropriate Entity management during the procurement process.	Verified Non-Disclosure Agreement of sampled vendor to determine that confidentiality commitments, are reviewed by appropriate Entity management during the procurement process.	No Exceptions Noted
	The entity has code of conduct within the Employee Handbook that establishes standards and guidelines for personnel ethical behaviour.	Inspected the code of conduct policies to determine that the entity has established standards and guidelines for personnel ethical behaviour including code of conduct.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	Personnel are required to read and accept the entity's code of conduct		
	All new employees have to read and sign the Confidentiality Agreement/NDA upon joining.	Selected a sample of new joiners and inspected personnel file to determine that Confidentiality agreements / NDA are signed.	No Exceptions Noted
	Agreements are established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties and subcontractors.	Selected a sample and inspected the vendor agreements to determine that the agreements define the terms, conditions and responsibilities of these vendors and their subcontractors.	No Exceptions Noted
	Customer can provide their issues, complaints or feedback through email to Business Heads. Employees can raise their complaints and grievances to HR.	Inspected customer resolution clauses in a sample of customer Statement of Work (SOW) and Client Contracts and determined that customer have a mechanism to communicate with the company.	No Exceptions Noted
CC1.2	**COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**		
	Management Review Meetings headed by CISO are held every year to discuss the security level, Internal Audit results, Risks, changes, technology trends, occurrence of incidents, and security initiatives.	Selected a sample of MRM meetings held and inspected the minutes to determine that MRM are held on a periodic basis.	No Exceptions Noted
	The Management team meets monthly and discuss the business as well as operational issues.	Selected a sample of management meetings held and inspected the minutes to determine that management meetings are held on a periodic basis.	No Exceptions Noted
CC1.3	**COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**		
	Organization charts are established that depicts authority, reporting lines and responsibilities for management of its information systems. These charts are communicated to employees and are updated as needed	Inspected the organization chart for an understanding of the hierarchy. Enquired with Management to determine that organisation charts are updated periodically.	No Exceptions Noted
	Company has Information security related policies and procedures that describes	Inspected ISMS Manual and related IT Policies to determine that these are documented approved.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	information security processes, practices and organization.		
	Information Security Policy & Procedures related to HR policies are reviewed and approved by the Management at least annually.	Inspected ISMS Manual and related IT Policies / HR Procedures to determine that changes during the audit period are approved by IT Head	No Exceptions Noted
	The responsibility of managing Information Security is assigned to CISO. Allocation of information security responsibility is documented in Roles and Responsibilities	Inspected Roles and Responsibilities document to determine that Information Security activities are responsibility of CISO.	No Exceptions Noted
CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**		
	The company has documented HR Policies and procedures including recruitment, training and exit procedures.	Inspected the HR Policies and procedures to determine that these are documented	No Exceptions Noted
	Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and transfer process.	Inspected the HR Policies and a sample of related job description to determined that requirements for each role are documented and are evaluated as part of the hiring process.	No Exceptions Noted
	New employees sign offer letter as their agreement and acceptance of broad terms of employment including a brief description of position and other terms.	Selected a sample of new joiners and inspected the appointment letter to determine that new joiners accept the terms of employment.	No Exceptions Noted
	Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings	Inspected Manpower Planning meeting invite to determine that resource planning is reviewed periodically.	No Exceptions Noted
	Internal HR Reference checks are conducted by HR team or the hiring manager through document verification and references checks with the former colleagues or managers provided in the resume. Negative Reference Checks require further management action. Third party verification is not being done	Selected a sample of new joiners and inspected personnel file to determine that internal HR reference checks are carried out as per defined policies.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	for every employee, but it is being done for employees where client demands it.		
	Newly hired personnel are provided sufficient training before they assume the responsibilities of their new position	Enquired with HR Head that all new employees undergo induction training.	No Exceptions Noted
	The induction training given by HR includes security training.	Inspected New Hire Induction Training Presentation to ensure that it includes policies on security. Selected a sample of new joiners and inspected the induction attendance/ training records (on GRC Platform) to determine that new joiners undergo information security trainings.	No Exceptions Noted
	An awareness refresher training on information security is provided to all employees on at least annual basis.	Inspected training records for a sample of employees and determined that annual training was completed.	No Exceptions Noted
CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**		
	All critical roles that are likely to have external or internal pressures report into the CEO/CTO	Inspected the Organization chart to determine that all critical roles that are likely to have external or internal pressures report into the CEO/CTO	No Exceptions Noted
	Job descriptions are reviewed by entity management on an annual basis as part of performance appraisals.	Inspected updated job descriptions to determine that job descriptions and roles and responsibilities are revised as an when required.	No Exceptions Noted
	Performance appraisals are performed at least annually.	Inspected HR Process Handbook to determine that Performance appraisals are performed at least annually.	No Exceptions Noted
	Communication and Information		
CC2.1	**COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**		
	Internal audits are performed, results are communicated, and corrective actions monitored.	Inspected a sample of internal audit reports & the corrective action taken to determine that an effective internal audit process is in place.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
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.**		
	System boundaries in terms of logical and physical boundaries are documented. Network diagrams are in place. System Boundaries are shared with the customers when it is required.	Inspected the ISMS Manual and the network diagram to determine that the Company has defined system boundaries.	No Exceptions Noted
	Customer responsibilities and appropriate system descriptions are provided in client contracts.	Inspected Client contracts for terms related to brief requirements of the system and customer responsibilities	No Exceptions Noted
	Security policies are published on shared directory and GRC Platform.	Inspected the shared directory and GRC Platform to determine that IT security policies available to internal users.	No Exceptions Noted
	An organizational wide incident management process is in place	Inspected Incident Management Procedures to determine inclusion of documented procedure for identifying incidents	No Exceptions Noted
	Entity communicates its commitment to security as a top priority for its customers via contracts.	Inspected client contracts of sampled customers to determine entity communicates its commitment to security as a top priority for its customers via contracts.	No Exceptions Noted
	All system changes that affect internal and external users are communicated in a timely manner	Inspected ISMS and related change management policies to determine how changes to system are communicated to users.	No Exceptions Noted
	External Client communication is carried out on a timely manner by the Project Manager or Lead using a standard client specific escalation matrix	Selected a sample of clients and inspected the escalation procedures to determine that these are established.	No Exceptions Noted
	Banners are provided on customer facing applications for communicating changes or downtime such as maintenance window	Enquired with management to determine that only major changes are communicated to clients through banners announcing changes or maintenance windows.	No Exceptions Noted
	CISO is responsible for decisions regarding changes in confidentiality practices and commitments. Operations team communicates these changes to the customers.	Enquired with CISO about procedures to authorize changes in confidentiality commitments and subsequent communication to customers.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	New employees hired at senior levels are communicated to stakeholders by HR through Email	Enquired that senior management hires are communicated internally and if necessary, externally.	No Exceptions Noted
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**		
	Company's security, availability and confidentiality commitments regarding the system are included in the client contracts and service agreements.	Inspected sample of Client SOW, MSA and NDA and determined that terms related to delivery of services are covered.	No Exceptions Noted
	Security policies are published on shared directory & GRC Platform.	Inspected the shared directory & GRC Platform to determine that IT security policies available to internal users.	No Exceptions Noted
	The induction training given by HR includes security training.	Inspected New Hire Induction Training Presentation to ensure that it includes policies on security. Selected a sample of new joiners and inspected the induction attendance/ training records (on GRC Platform) to determine that new joiners undergo information security trainings.	No Exceptions Noted
	Customer responsibilities are described in client contracts.	Inspected a sample of client contracts to determine explicit responsibilities of customer	No Exceptions Noted
	Users are informed of the process for reporting complaints and security breaches during induction Security Training.	Selected a sample of new employees and inspected evidence to determine that they attended Security Training during induction.	No Exceptions Noted
	Customer can provide their issues, complaints or feedback through email to Business Heads. Employees can raise their complaints and grievances to HR.	Inspected customer resolution clauses in a sample of customer Statement of Work (SOW) and escalation matrix and determined that customer have a mechanism to communicate with the company.	No Exceptions Noted
	A client escalation matrix is in place to ensure that communication channels for external users are available.	Inspected the client escalation mechanism to determine that it is implemented	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	Customer responsibilities are described in the customer contracts and in system documentation	Inspected a sample of customer SOW for the roles and responsibilities and determined that roles and responsibilities are clearly defined. .	No Exceptions Noted
	CISO is responsible for decisions regarding changes in confidentiality practices and commitments. Operations team communicates these changes to the customers.	Enquired with CISO about procedures to authorize changes in confidentiality commitments and subsequent communication to customers.	No Exceptions Noted
	Changes to system boundaries, network systems are communicated to clients, if it impacts their operations	Enquired with CISO that system boundaries, network systems are communicated to clients, if it impacts their operations.	No Exceptions Noted
	Incidents impacting external users are communicated to them through emails along with root cause analysis, if required.	Enquired with CISO that Incidents impacting external users are communicated to them through emails along with root cause analysis, if required.	No Exceptions Noted
	Risk Assessment		
CC3.1	**COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**		
	Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk. This is part of the Risk Management Framework.	Inspected Risk Assessment and Risk Treatment procedure to determine that Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk.	No Exceptions Noted
	Risk Assessment and Risk Treatment Procedure related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment and Risk Treatment Procedure to determine that the Company has a defined and documented risk assessment process.	No Exceptions Noted
	Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings	Inspected a sample of Manpower Planning sheet to determine that resource planning is reviewed periodically.	No Exceptions Noted
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.**		
	Risk Assessment and Risk Treatment Procedure related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment and Risk Treatment Procedure to determine that the Company has a	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
		defined and documented risk assessment process.	
	A risk assessment is performed annually or whenever there are changes in security posture. As part of this process, threats to security are identified and the risk from these threats is formally assessed.	Inspected Risk Assessment and Risk Treatment performed during the audit period to determine updating of asset inventory, threats and risks and to determine that risk assessment is carried out at least on an annual basis.	No Exceptions Noted
	Identified risks are rated and get prioritized based on their likelihood, impact, priority and the existing control measures.	Inspected Risk Assessment performed during the year to determine identified risks are rated	No Exceptions Noted
	All information assets are identified in an asset inventory	Inspected the Asset Inventory to determine that all information assets are identified in an asset inventory.	No Exceptions Noted
	Monitoring tools Grafana is implemented to detect control issues - CPU Usage, Drive Space, Memory Usage and Uptime.	Inspected the Azure Monitor and Grafana screens to determine it is implemented to detect control issues - CPU Usage, Drive Space, Memory Usage and Uptime.	No Exceptions Noted
CC3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**		
	The IT department maintains an up-to-date listing of all software and the security patches related to OS and application and patches are applied manually after testing in QA Environment.	Inspected patching maintenance sheet to determine that patches are applied periodically.	No Exceptions Noted
	List of all hardware is maintained as part of asset register.	Inspected the asset register list to determine that all assets are recorded.	No Exceptions Noted
	Company has defined a formal Risk Assessment and Risk Treatment procedure for evaluating risks based on identified Probability, Impact, Risk Rating, Risk Priority and mitigating controls.	Inspected Risk Assessment and Risk Treatment procedure to determine that the Company has a defined and documented risk assessment process.	No Exceptions Noted
CC3.4	**COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**		
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed by appropriate Entity management during the procurement process.	Inspected Non-Disclosure Agreement of sampled vendor to determine that confidentiality commitments, are reviewed by appropriate Entity management during the procurement process.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	Monitoring Activities		
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 internal audit function conducts system security reviews monthly by rotating different areas. Results and recommendations for improvement are reported to management.	Inspected a sample of internal audit reports & the corrective action taken to determine that internal audits and system reviews are performed periodically.	No Exceptions Noted
	IT system access is reviewed on a annually basis.	Inspected the information security policies containing access controls to determine that these are documented. Inspected Internal Audit Report to determine that access rights are reviewed regularly, and user access lists are reconciled against active HR records.	No Exceptions Noted
	Vulnerability assessment & penetration tests of Network are performed annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions Noted
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 internal audit function conducts system security reviews monthly by rotating different areas. Results and recommendations for improvement are reported to management.	Inspected a sample of internal audit reports & the corrective action taken to determine that internal audits and system reviews are performed periodically.	No Exceptions Noted
	Security Groups (equivalent of Virtual Firewall) is configured on production instances on Azure.	Inspected the Security group configuration settings of production instances to determine that the inbound and outbound rules are configured.	No Exceptions Noted
	IT system access is reviewed on a annually basis.	Inspected the information security policies containing access controls to determine that these are documented. Inspected Internal Audit Report to determine that access rights are	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
		reviewed regularly and user access lists are reconciled against active HR records.	
	Vulnerability assessment & penetration tests of Network are performed annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions Noted
	Results of the vulnerabilities and internal external tests are reviewed by the management	Enquired with CISO that Results of the vulnerabilities and internal external tests are reviewed by the management	No Exceptions Noted
	All internal audit issues are tracked until closure to ensure that these are closed.	Inspected the Internal Audit results that issues are tracked until closure to ensure that these are closed.	No Exceptions Noted
	Control Activities		
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.**		
	Vulnerability assessment & penetration tests of Network are performed annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions Noted
	Internal audits including access reviews are performed every month. Results and recommendations for improvement are reported to management.	Inspected sample of monthly audit reports to determine that audits are performed periodically.	No Exceptions Noted
	Segregation of duties is in place for critical functions and departments	Inspected Roles and Responsibilities document to determine that Segregation of duties are in place.	No Exceptions Noted
CC5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**		
	Vulnerability assessment & penetration tests of Network are performed annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions Noted
	Internal audits including access reviews are performed every month. Results and	Inspected monthly audit reports (covering different areas) to	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	recommendations for improvement are reported to management.	determine that audits are performed periodically	
	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment & Treatment Procedure to determine that the Company has a defined and documented risk assessment process.	No Exceptions Noted
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.**		
	Escalation procedures are defined at relevant places within the policies for policy Exceptions,	Inspected client escalation matrix to determine that escalation procedure is in place.	No Exceptions Noted
	All policies and procedures clearly define the roles, responsibilities and accountability for executing policies and procedures.	Inspected the job descriptions, roles & responsibilities to determine that these are defined in written job descriptions.	No Exceptions Noted
	Logical and Physical Access Controls		
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.**		
	Company has documented procedure for logical access controls	Inspected the access control policy and procedure and determined that these are documented.	No Exceptions Noted
	Access is granted on least privileges basis as default and any additional access needs to be approved.	Inspected access control procedure document and determined that access is granted on least privileges basis as default and any additional access needs to be approved.	No Exceptions Noted
	Company has established hardening standards production infrastructure that include requirements for implementation of security groups, access control, configuration settings, and standardized policies.	Inspected IT policies and procedures to determine that hardening standards have been established.	No Exceptions Noted
	Production hosts and Security Groups (which are the equivalent of Firewalls) are hardened according to Industry best practices. Only the required ports are opened for inbound access at the load balancer level.	Inspected Azure settings to determine that VPC has been setup and all production servers are within the private subnet. Inspected the IAM settings and security groups to determine that	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
		only the production group has access to production resources.	
	3rd party vulnerability scans of Visionify are performed at least annually and their frequency is adjusted as required to meet ongoing and changing commitments and requirements.	Inspected the most recent VA reports from external agency to determine that VA are carried out and that these are discussed in management meetings.	No Exceptions Noted
	Company does not allow customers or external users to access its systems.	Enquired with IT team that external users cannot access company's network systems	No Exceptions Noted
	The company does not have Active Directory. Azure IAM is used for logical access control on Azure.	Enquired with IT Head that company does not have Active Directory and Azure logical access control is through IAM. Observed a user sign-on process to determine if an ID and password were required to verify identity for logging to Azure through MFA.	No Exceptions Noted
	Cloud infrastructure are configured to use the Azure's identity and access management system (IAM) . Relevant groups have been added in IAM.	Inspected the IAM settings and security groups to determine that several groups have been formed for different teams and only the production group has access to production resources.	No Exception Noted
	Direct access to cloud infrastructure is possible only through encrypted SSH access by the IT team.	Inspected the properties of VPC security group and determined that the inbound connection to instances in the VPC is set to be accessed by an SSH connection.	No Exceptions Noted
	For Azure console access, Multi Factor Authentication is implemented.	Inspected the user settings in Azure console for the production group members to determine that multifactor authentication has been enabled.	No Exceptions Noted
	The IT department maintains an up-to-date listing of all software.	Inspected the software list maintained by the IT to ensure that it is up to date. Inspected the software installed in sample desktop to ascertain that current versions are installed.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	All Assets are assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed.	Inspected the asset register and determined that assets and their owners are clearly documented.	No Exceptions Noted
	Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by Team Lead and IT Head and reviewed by IT on a periodic basis.	Inspected screenshots of Azure IAM to determine that administrator privileges for the domain were limited to IT team and privileged user.	No Exceptions Noted
	Account sharing is prohibited unless approved by management.	Inspected Access Control procedure about account sharing and determined that it is prohibited unless authorized in writing.	No Exceptions Noted
	Password policy is set at the Local Policy level. Passwords are manually set on each user's desktops by the IT team. These are 7 characters in length with complexity enabled. Passwords are reset by the IT team manually every 45-60 days by going to each user's desktop and resetting the passwords. On the next login, the user in the presence of the IT team will reset the password.	Enquired with the IT Head that passwords are manually set by the IT team and are reset every 45-60 days by the IT team.	No Exceptions Noted
	Access to data is restricted to authorized applications through Azure IAM. Access to Company systems is given only against authorization. Access given to new employees is one of least privileges.	Inspected Azure IAM and determined that access requires a combination of user ID and unique password.	No Exceptions Noted
	Employees don't have access to printers or any other output device. Printer access is given for few teams such as HR and Finance.	Enquired with IT team that no printer access is given to employees and determined based on enquiry that output access is controlled.	No Exceptions Noted
	All confidential data is classified as per the data classification policy.	Inspected information security policies to determine that data classification policies are documented.	No Exceptions Noted
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.**		

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	On the day of joining, HR will send a mail to the IT Help desk providing the details of the new joiners. The IT then provides necessary access as per the request. Employee user accounts are removed from various applications and network systems as of the last date of employment manually based on access revocation requests sent by the HR department.	Inspected the Access Control procedure and determined that granting, modifying, or deactivating access is only done against written authorization. Inspected access request forms/emails for a sample of employees to determine that written authorization is in place. Inspected access revocation request /exit checklist for a sample of employees to determine that written authorization for deactivation is in place.	No Exceptions Noted
	When an employee leaves the organization, the employee's manager initiates the 'Exit Process'. HR informs respective teams / IT teams within 24 hours to deactivate/delete the user ID from the email system and all applications. An exit checklist is used to ensure compliance with termination procedures.	Selected a sample of exited users and inspected Email from HR to IT and Exit Checklist to determine that the exit process and related account deactivation is as per defined procedures. Inspected Azure IAM to determine that the exited user has disabled status.	No Exceptions Noted
	Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by Team Lead and IT Head and reviewed by IT on a periodic basis.	Inspected screenshots of Active Directory to determine that administrator privileges for the domain were limited to IT team and privileged user. Selected a sample of requests for privileged access and Inspected the authorization email to determine that privileged access is authorized by Team Lead and IT Head.	No Exceptions Noted
	Company does not allow non-employees to access its systems.	Enquired with IT staff about access to non-employees.	No Exceptions Noted
	Password policy is set at the Local Policy level. Passwords are manually set on each user's desktops by the IT team. These are 7 characters in length with complexity enabled. Passwords are reset by the IT team manually every 45-60 days by going to each user's desktop and resetting the passwords. On the next login, the user in	Enquired with the IT Head that passwords are manually set by the IT team and are reset every 45-60 days by the IT team.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	the presence of the IT team will reset the password.		
	Company does not employ contractors in its offices.	Enquired with IT staff about access to non-employees to determine that there are no contractors.	No Exceptions Noted
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.**		
	A role based security process has been defined with in Azure infrastructure based on job requirements.	Inspected the Azure console screens to determine that security groups based on departments and roles have been defined	No Exceptions Noted
	IT system access is reviewed on a annually basis.	Inspected the information security policies containing access controls to determine that these are documented. Inspected Internal Audit Report to determine that access rights are reviewed regularly, and user access lists are reconciled against active HR records.	No Exceptions Noted
	Company does not allow reactivation of ID belonging to an exited employee.	Enquired with IT Head that reactivation of IDs it is prohibited.	No Exceptions Noted
	Account sharing is prohibited unless approved by management.	Inspected Access Control procedure about account sharing and determined that it is prohibited unless authorized in writing. Inspected a system generated list of user accounts to determine that shared accounts do not exist	No Exceptions Noted
CC6.4	**The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.**		
	Entry to all office premises is restricted to authorized personnel. Physical access control system has been implemented to secure the facilities.	Observed that the entry to premises is restricted by physical security and access control.	No Exceptions Noted
	Physical access to office premises is monitored through CCTV installed at key points within the premises.	Observed that the CCTV are located at entry exit only which is working fine	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
		There is no camera installed inside the office premise.	
	There is a security desk at the office entry manned by a security guard	Observed the security staff at the reception who ensure that all visitors and employees are screened before entering the office.	No Exceptions Noted
	All visitors have to enter their details in the visitor register.	Inspected the visitor register for a sample of dates to determine that visitor register is maintained.	No Exceptions Noted
	Visitor badges are for identification purposes only and do not permit access to the facility.	Observed that visitor badges are for identification purposes only and do not permit access to any secured areas of the facility.	No Exceptions Noted
	All visitors must be escorted by a Company employee when visiting office facilities.	Observed that all visitors are escorted by a Company employee when visiting Company office.	No Exceptions Noted
	ID cards that include an employee picture must be worn at all times when accessing or leaving the facility.	Observed a sample of employees that employees wear picture IDs at all times.	No Exceptions Noted
	Physical access is setup by the HR Dept for new joiners after all HR formalities are completed. ID cards by default does not have access to any of the sensitive areas.	Selected a sample of new employees and inspected that the access rights were granted in the physical access system only to authorised new joiners.	No Exceptions Noted
	Physical access to sensitive areas / server rooms is granted only to privileged users / IT Team Access to such restricted zone is given against written request by the CTO.	Inquired with IT Team that access to server room and other sensitive areas is granted only to IT team.	No Exceptions Noted
	A periodic review of physical access to sensitive areas against active employee list is carried out by IT.	Inspected a sample of access review reports for sensitive areas to determine that access rights are reviewed regularly.	No Exceptions Noted
	Upon the last day of employment, HR Team sends exit email requesting for deactivation of physical access for terminated employees. Physical access is deactivated by the Admin Team	Inspected system to determine that the employee ID numbers for the sample of exited employees were deleted from the electronic access control system.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	Employees are required to complete their exit clearance process on the last day, and all access are disabled.	Inspected the exit checklist for a sample of terminated employees to determine that access is disabled. Inspected the electronic access control system activation / deactivation log to ensure that access of terminated employees have been revoked.	No Exceptions Noted
	On a quarterly basis, Internal audit / HR performs a reconciliation that physical access for terminated employees has In fact been deactivated in the physical access system.	Selected a sample of quarters and inspected physical access reviews to determine that physical access reviews / reconciliations are performed periodically.	No Exceptions Noted
	No contractor is given physical access or electronic access control device.	Enquired with facilities about contractor access and determined no contractor has been given physical access for entering the office.	No Exceptions Noted
	The sharing of access badges and tailgating are prohibited by policy.	Observed that access badges are not shared & no tailgating observed.	No Exceptions Noted
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.**		
	Media Handling Policy is implemented for procedures relating to disposal of information assets / equipment	Inspected Data Deletion Policy to determine that Media Handling Policy is implemented for procedures relating to disposal of information assets / equipment	No Exceptions Noted
	All data is erased from laptops and other media prior to destruction disposal	Enquired with IT Head that all data is erased from laptops and other media prior to destruction disposal	No Exceptions Noted
CC6.6	**The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**		
	The production system at Azure is protected by security groups rules (virtual firewall) set up for the virtual private cloud (VPC) provided by Azure. VPC is used to protect all Production system hosted at Azure.	Inspected Azure settings to determine that VPC has been setup and direct access to production instances is only through 2048 bit SSH keys.	No Exceptions Noted
	Access to modify security group rules is restricted by IT Head to Administrators.	Inspected the user list on IAM to determine that access to modify	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
		security group rules is restricted to Administrators/IT team.	
	Use of removable media is not prohibited.	Inspected it as a risk in risk register to determine that usage of removable media is not controlled.	No Exceptions Noted.
	Connections to the Azure-hosted servers are through authenticated SSH sessions or authenticated secure browser session using HTTPS.	Inspected Azure settings to determine that direct access to production instances is only through SSH keys.	No Exceptions Noted
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.**		
	Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted.	Inspected the information security policies to determine that transmission of sensitive information over the internet happens only when the information is encrypted.	No Exceptions Noted
	External users access applications hosted at cloud infrastructure (Azure) through secure https with SSL/TLS certificates.	Inspected evidence for implementation of https encryption to determine that secure https connections are used.	No Exceptions Noted
	Use of removable media is not prohibited.	Inspected it as a risk in risk register to determine that usage of removable media is not controlled.	No Exceptions Noted.
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.**		
	Antivirus software is installed on workstations, laptops, and servers. This system provides antivirus system scans and endpoint protection.	Inspected a sample of Laptops and determined that antivirus is installed, and signature files were updated.	No Exceptions Noted
	The ability to install software on workstations and laptops is restricted to IT support personnel through admin accounts.	Inspected the Information Security Policies to determine that users are not allowed to install any software.	No Exceptions Noted
	Any viruses discovered are reported to IT team either by the antivirus system or by the affected employees.	Inspected the antivirus console for configuration details about updating and alerts.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	System Operations		
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.**		
	Management has defined configuration standards and hardening standards.	Inspected the System Hardening Checklist to determine that Management has defined configuration standards and hardening standards.	No Exceptions Noted
	The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	Inspected the Grafana dashboard to determine entity monitors infrastructure and software for noncompliance with the standards.	No Exceptions Noted
	Vulnerability assessment & penetration tests are performed annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions Noted
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.**		
	Hardening Checklists are in place for hardening of IT infrastructure/desktops.	Inspected the System Hardening Checklist to determine that Management has defined configuration standards and hardening standards.	No Exceptions Noted
	IT team receive requests for support through phones, emails and Azure Boards Ticketing tool which may include requests to reset user passwords etc.	Inspected a sample of IT support ticket emails reported by users to determine that support tickets are logged as Azure Boards Ticket.	No Exceptions Noted
	Vulnerability assessment & penetration tests are performed annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions Noted
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.**		
	A formal, defined incident management Policy is documented as part of	Inspected Incident Management Policy to determine that incident	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	Information Security Policies for evaluating reported events.	management process is documented.	
	Incidents are reported to the IT team by phone or email. These are tracked through Incident log on Excel.	Inspected the screenshot of the incident log to determine that incidents are tracked.	No Exceptions Noted
	Reported incidents are logged in Excel/Incident form and include the following details Incident Type Data and Time of incident Details Action Taken Root Cause (For select high risk incidents)	Inspected a sample of incident report to determine that incidents covered Incident Type, Data and Time of incident, Details, Action Taken, Root Cause as per defined process.	No Exceptions Noted
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.**		
	All security incidents are also reviewed and monitored by the Information Security Group. Corrective and preventive actions are completed for incidents.	Inspected minutes of ISG committee meeting minutes to determine that discussion on incidents takes place.	No Exceptions Noted
	Change management requests are opened for events that require permanent fixes.	Inspected Incident Management Procedure and determined that for some incidents, change requests are opened as part of resolution.	No Exceptions Noted
	All incidents are evaluated and necessary action taken to closure the threat / vulnerability	Inspected Incident Management Procedure and determined that necessary action is taken to close the threat/vulnerability.	No Exceptions Noted
	Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.	Inspected Incident Management Procedure and determined that necessary action is taken for communicating security incidents and actions taken to affected parties are developed and implemented	No Exceptions Noted
	Quarterly, management reviews all incidents that occurred during the month is conducted and headed by CISO.	Inspected MRM Meeting minutes to determine that monthly management reviews all incidents that occurred during the quarter is conducted.	No Exceptions Noted
	HR policies include code of conduct and disciplinary policy for employee misconduct.	Inspected the Employee Handbook for Code of Conduct and Disciplinary Policy	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
CC7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**		
	All incidents are evaluated and necessary action taken to closure the threat / vulnerability.	Inspected Incident Management Procedure and determined that necessary action is taken to close the threat/vulnerability.	No Exceptions Noted
	Root cause analysis is performed for major incidents.	Inspected the screenshot of the incident log and related root cause description for some incidents to determine that incidents are tracked.	No Exceptions Noted
	Change Management		
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.**		
	System and regression testing is prepared by the testing department using approved test plans and test data.	Inspected test plans for sample of releases to determine that test plans included steps for regression testing, security testing.	No Exceptions Noted
	Software code is maintained in GitHub.	Inspected screenshot of GitHub server to determine that software code is maintained in GitHub.	No Exceptions Noted
	Software development changes are tested through unit testing and QA testing followed by UAT. Each of these changes are captured & monitored in change requests. Test plans used for testing QA team.	Inspected a sample of changes for software development to determine that QA/UAT testing is carried out.	No Exceptions Noted
	There is a formal release process for releasing builds. Release notes contain what all is released in the release. The testing team does the complete testing of the release. On receipt of sign off mail from the testing team the release is deployed on production servers.	Selected a sample of releases during the audit period and inspected the release notes and the related approval to determine that all releases are tested and approved before deployment.	No Exceptions Noted
	Separate environments are used for development, testing, and production. Developers do not have the ability to make changes to software in testing or production.	Enquired with the IT Head to determine that separate environments are maintained for development, testing and production and also to understand about process to carry out major changes.	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	All change requests are submitted with Risk Assessment, implementation and rollback plans. Code repository & deploy tool has a turnover process that includes back out steps commit is to be reverted.	Inspected a sample of change requests to determine that they had Risk Assessment, implementation and rollback plans included.	No Exceptions Noted
	Changes are communicated to the appropriate client and user community if the change has any potential impact on the user base.	Enquired with IT Head that changes are communicated to clients and end users if it has impact on those users.	No Exceptions Noted
	The change management policy has defined roles and assignments thereby providing segregation of roles in the change management process.	Inspected the Change Management Policy and Procedures to determine that these define segregation of roles for change management.	No Exceptions Noted
	Entity has defined its change management and approval processes in its information security policies.	Inspected Information Security Policy and determined that change management policy and procedures are defined.	No Exceptions Noted
	Software design and development change procedures are documented in the Change Management and Control Policy.	Inspected the Change Management and Control Policy to determine that software design and development change procedures are documented.	No Exceptions Noted
	All change requests are logged and change request ticket created.	Selected a sample of change requests to determine that these are logged and that changes are approved by IT Head.	No Exceptions Noted
	A risk assessment is performed on a periodic basis. The risk assessment includes identifying potential threats and assessing the risks associated with identified. Change requests are created based on the identified needs.	Inspected the risk management procedures to determine if change requests are created based on identified needs.	No Exceptions Noted
	Risk Mitigation		
CC9.1	**The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**		
	Entity has a documented Business Continuity Procedure & Plan including Disaster Recovery guideline to be used in the event of an event necessitating systems infrastructure recovery.	Inspected the Business Continuity Procedure & Plan to determine that a plan and procedure has been documented with clear	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
		responsibilities on those required to respond.	
	Business continuity and disaster recovery plans, including restoration of backups, are tested quarterly.	Inspected the Business Continuity Planning Policy and determined that BCP plans are tested annually.	No Exceptions Noted
CC9.2	**The entity assesses and manages risks associated with vendors and business partners.**		
	New Third-Party Service Providers are selected based on a Vendor Selection Process. Security risk assessment is a key part of the vendor selection process. Company requires all key subservices to be compliant with security certifications and attestations such as ISO 27001, SOC1 or SOC2.	Enquired with Management that vendors and third-party service providers are selected based on a vendor due diligence. Enquired with Management that there was no material third party vendor that was onboarded during the audit period.	No Exceptions Noted
	Company obtains and reviews compliance reports and certificates such as PCI DSS, ISO 27001, SOC1 or SOC2 for its key vendors. Opinion section and relevant controls are reviewed for any Exceptions. This is part of vendor monitoring.	Inspected SOC2 attestation reports of Company's vendors (Azure) to determine that the company receives such reports that are used in monitoring controls.	No Exceptions Noted
	A formal contract is executed between Company and Third-Party Service Providers before the work is initiated. Agreement includes terms on confidentiality, responsibilities of both parties.	Inspected a sample of vendor contracts to determine that vendors contracts are in place.	No Exceptions Noted
	All customer & vendor contracts have terms related to confidentiality.	Inspected an NDA and vendor contracts to determine that it contains clauses relating to confidentiality.	No Exceptions Noted
	A confidentiality agreement is signed by all employee at the time of joining. In addition, NDAs are signed with third parties wherever required.	Inspected the confidentiality agreement template to determine that agreements include terms on confidentiality and non-disclosure.	No Exceptions Noted
	Vendor systems are subject to review as part of the vendor risk selection. Azure is the sole service provider that provides data center services. Attestation reports (SOC 2 reports) are obtained from Azure and evaluated when available.	Enquired with management that they have obtained and reviewed SOC2 report for Azure .	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
	ADDITIONAL CRITERIA FOR AVAILABILITY		
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.**		
	Processing capacity for cloud infrastructure for Azure is monitored by Zabbix and Grafana on an ongoing basis.	Inspected Zabbix and Grafana settings to determine that alerts & thresholds have been setup for abnormal conditions such as low CPU utilization, network outage, free storage, etc.	No Exceptions Noted
A1.2	**The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.**		
	Environmental controls (fire extinguishers, fire sprinklers and smoke detectors) have been installed to protect perimeter area. CCTV are installed at key points for surveillance. Devices are checked on a periodic basis and checklists are prepared.	Observed that fire extinguisher across all office premises that these are in working condition.	No Exceptions Noted
	Fire drill is conducted annually.	Observed the fire drill report and verified that there were no exceptions noted.	No Exceptions Noted
	Uninterruptible power supply (UPS) devices are in place to secure critical IT equipment against power failures and fluctuations.	Observed the UPS installed at the premises to determine that they are in good working condition.	No Exceptions Noted
	Company has multiple ISPs in place to provide redundancy in case of link failure	Inspected the network diagram to determine that the company has multiple ISPs in place.	No Exceptions Noted
	Vendor warranty specifications are complied with and tested to determine if the system is properly configured.	Inspected MSAs, building lease and vendor contract for maintenance of various environmental controls.	No Exceptions Noted
	Facilities and admin personnel monitor the status of environmental protections on a regular basis. Maintenance checklists are used where applicable.	Inspected environmental control check report and determined that maintenance reviews are carried out. Inspected the UPS preventive maintenance reports, vendor maintenance contracts to determine	No Exceptions Noted

Ref. #	Controls implemented by Visionify	Test Procedures	Test Results
		that preventive maintenance is performed periodically.	
	Backup policy is defined in the information security policies.	Inspected information security policies to determine that backup schedules, frequency of backups are documented.	No Exceptions Noted
	Automated backup systems are in place to perform scheduled differential and full back up of production systems and internal office data.	Inspected screenshots of the backup systems to determine that backups are scheduled to be taken on a regular basis.	No Exceptions Noted
A1.3	**The entity tests recovery plan procedures supporting system recovery to meet its objectives.**		
	Business Continuity Plan and Procedure including Disaster recovery for various disruption scenarios are documented.	Inspected Business Continuity Plan and Procedure to determine that these are documented.	No Exceptions Noted
	Business continuity plans, including restoration of backups, are tested at least quarterly.	Inspected BCP/DR test report to determine that BCP plans have been tested.	No Exceptions Noted
	ADDITIONAL CRITERIA FOR CONFIDENTIALITY		
C1.1	**The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.**		
	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	Inspected the Data Protection and Security policy to determine that the Company retains information as per the defined policies.	No Exceptions Noted
C1.2	**The entity disposes of confidential information to meet the entity's objectives related to confidentiality.**		
	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	Inspected the Data Protection and Security policy to determine that the Company destroys or disposes of confidential information as per the defined retention policies.	No Exceptions Noted
	Security policies are published on shared directory and GRC Platform.	Inspected the shared directory and GRC Platform to determine that IT security policies available to internal users.	No Exceptions Noted

SECTION 5

Other Information Provided by Visionify Inc.

Other Information Provided by Visionify Inc.

The information provided in this section is provided for informational purposes only by Visionify . Independent Auditor has performed no audit procedures in this section.

Disaster and Recovery Services

The AICPA has published guidance indicating that business continuity planning, which includes disaster recovery, is a concept that addresses how an organization mitigates future risks as opposed to actual controls that provide user auditors with a level of comfort surrounding the processing of transactions. As a result, a service organization should not include in its description of controls any specific control procedures that address disaster recovery planning. Therefore, Visionify disaster recovery plan descriptions of control procedures are presented in this section.

In addition to the physical controls, Visionify has implemented logical controls to safeguard against interruption of service. Visionify has developed a number of procedures that provide for the continuity of operations in the event of an availability zone failure by spinning up multiple servers across all availability zones in Azure.

The disaster recovery plan defines the roles and responsibilities and identifies the critical IT application programs, operating systems, personnel, data files, and time frames needed to ensure high availability and system reliability based on a business impact analysis.