JASCI SOFTWARE SOC 2 TYPE 2 REPORT

Statement of Confidentiality

The information contained in this SOC 2 Type 2 Report is confidential and intended solely for the use of the JASCI Software. This report may not be disclosed, copied, or distributed, in whole or in part, without the prior written consent of the organization that commissioned the audit, except as required by law or regulation.

The contents of this report are to be used exclusively for the purpose of assessing the organization's internal controls over the Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, and Privacy). The recipient agrees to take all reasonable precautions to protect the confidentiality of the information and to prevent its unauthorized use or disclosure.

By accepting this report, the recipient acknowledges and agrees to the terms of this confidentiality statement.

Table of Contents

SECTION 1: INDEPENDENT SERVICE AUDITORS' REPORT

Section 1: Independent Service Auditors' Report

Independent Service Auditors' Report on Description of JASCI Software. System and the Suitability of the Design and Operating Effectiveness of Controls relevant to Security, Availability, Confidentiality, Trust Service Principles.

1.1 To the JASCI Software Management Scope

We have reviewed the system description for JASCI Software this engagement covers JASCI's next generation cloud-based Warehouse Management Platform, designed for the logistics industry. Covering the period of **01st December 2024 to 31st March 2025**. This examination was conducted based on the guidelines outlined in the Description Criteria DC Section 200 (2018) for SOC 2 reports. We assessed the design and operational effectiveness of the controls mentioned in the description to ensure that JASCI Software's service commitments and system requirements would meet the relevant Trust Services Criteria for security, availability, and confidentiality, as defined in TSP Section 100 (2017).

1.2 JASCI Software Responsibilities

JASCI Software is accountable for its service commitments and system requirements, as well as for designing, implementing, and maintaining effective controls within the system. This is to ensure that those commitments and requirements are met. JASCI Software has submitted an assertion titled "Management of JASCI Software's Assertion," which outlines the presentation of the system description according to the Description Criteria. It also addresses the suitability of the design and operational effectiveness of the controls described. This assertion aims to provide reasonable assurance that, if these controls operate effectively, the service commitments and system requirements will be fulfilled based on the applicable Trust Services Criteria.

1.3 Service Auditors' Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examinations were conducted in accordance with attestation standards established by the **American Institute of Certified Public Accountants (AICPA)** issued by the Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period of 01st December 2024 to 31st March 2025. An examination of description about a service organization's system and the suitability of the design and operating effectiveness of its controls to achieve the related control objectives stated in the description involves:

- **Performing** procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description.
- **Assessing** the risk in case the description is not fairly presented or that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- **Testing** the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- **Evaluating** the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section 3 of this report.

We believe that the evidence we obtained were sufficient and appropriate to provide a reasonable basis for our opinion.

The examination includes a detailed review of the description provided by the service organization. This involves assessing the accuracy and completeness of the system description to ensure it fairly represents the services, controls, and processes in place. We evaluate:

- The system boundaries are clearly defined.
- The services provided by the organization are accurately described.
- Key components such as infrastructure, software, people, and data are appropriately detailed.

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the Statements on Quality Control established by the AICPA and, accordingly, maintained a comprehensive system of quality control.

1.4 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 its 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 or 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.

1.5 Opinion

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

a) The Description fairly presents the system that was designed and implemented throughout the period of 01st December 2024 to 31st March 2025.
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 of 01st December 2024 to 31st March 2025 and process applied the controls contemplated in the design of the Service Organization's controls throughout the period of 01st December 2024 to 31st March 2025.

1.6 Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section IV of the report.

1.7 Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is, intended solely for the information and use of JASCI Software , user entities of the system related to SOC services provided to its customers relevant to the Security, Availability, Processing Integrity and Confidentiality and system of JASCI Software during some or all of the period 01st December 2024 to 31st March 2025 and 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, and other parties
- Internal control and its limitations
- 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.

Shreyash Singwala

Shreyash Singwala, Certified Public Accountant

License No: PAC-CPAP-LIC-034059

Date: 31-03-2025

SECTION 2: MANAGEMENT'S ASSERTION PROVIDED BY SERVICE ORGANIZATION

JASCI Software Management's Assertion SOC 2 Type 2 Report

Report Period: 01st December 2024 to 31st March 2025

Assertion by Management:

JASCI Software management is responsible for designing, implementing, and maintaining effective controls to meet the Trust Services Criteria as outlined by the AICPA.

We assert that, during the period from 01st December 2024 to 31st March 2025, JASCI Software maintained controls that were effectively designed and operated to provide reasonable assurance that the control objectives related to the Trust Services Criteria were met.

Control Environment and Framework:

Our control framework is based on industry best practices and is designed to ensure compliance with the **SOC 2 Type 2** requirements. The following measures were implemented to support the criteria:

1. **Security:** Implementation of access controls, encryption, logging, and monitoring to protect information from unauthorized access.
2. **Availability:** Redundant infrastructure, incident management, and disaster recovery mechanisms to ensure service uptime.
3. **Processing Integrity:** Systematic quality assurance measures and data validation to maintain processing accuracy.
4. **Confidentiality:** Data classification and encryption policies ensuring protection of sensitive information.
5. **Privacy:** Compliance with regulatory privacy requirements, including data handling and user consent mechanisms.

Independent Auditor's Examination:

An independent third-party auditor conducted an assessment of our controls based on **SOC 2 Type 2** standards. The auditor's report details the effectiveness of controls and confirms our adherence to the Trust Services Criteria.

Name: Al Falack (Chief operating Officer)

Signature: 

Date: 31/03/25

SECTION 3: DESCRIPTION OF THE SYSTEM

3.1 System Description Provided by Service Organization

Location of JASCI Software office
44 Executive Blvd., Suite 201, Elmsford, NY 10523

3.2 Description of Control Environment, Control Activities

3.2.1 Control Environment

The security, availability, confidentiality, categories, and applicable trust Services criteria were used to evaluate the suitability of the design of controls stated in the description.

3.2.2 Organization Roles and Responsibilities

Authorities and Responsibilities

JASCI Software has demonstrated compliance with organizational management practices by maintaining a well-defined Organization Chart, reflecting a clear structure and hierarchy to support efficient governance and communication within the company.

3.2.3 Policies and Procedures

JASCI Software maintains documented policies and procedures for each organizational unit in scope. These policies and procedures define approaches, rules, and guides for business processes to support their effectiveness, efficiency, reliability, and compliance with legislative and contractual requirements. Policies and procedures are reviewed in case of internal business changes or external environments. JASCI Software has established and implemented policies and procedures based on leading international practices

3.2.3.1 Access Control

During the audit of JASCI Software's Oracle Cloud environment, it was observed that access to cloud resources is appropriately provisioned based on job responsibilities, adhering to the principle of least privilege. This ensures that users have only the necessary access rights required for their roles, minimizing potential security risks. Furthermore, Multi-Factor Authentication (MFA) is enforced for all sensitive systems within Oracle Cloud, significantly enhancing protection against unauthorized access. The implementation of Role-Based Access Control (RBAC) was also verified, restricting access according to defined user roles and ensuring that permissions are accurately aligned with business needs. This access control framework demonstrates JASCI Software’s strong commitment to safeguarding its cloud infrastructure.

3.2.3.2 Data Classification and Handling

During the audit of JASCI Software's data management practices, it was confirmed that data is classified into clear categories: Public, Internal, Confidential, and Restricted, with sensitive data handling practices tailored to these classifications. Confidential and Restricted data are subject to stringent security measures, including encryption and secure storage, ensuring that access is strictly limited to authorized personnel only. The company demonstrated a robust approach to data retention, ensuring compliance with business and legal requirements. Additionally, secure disposal methods are employed to guarantee proper data destruction when data is no longer needed, aligning with best practices for data security and regulatory compliance

3.2.3.3 Encryption

During the audit of JASCI Software's use of Oracle Cloud, it was observed that the company effectively utilizes Oracle Cloud's encryption services to encrypt data at rest, employing FIPS 140-2 validated encryption algorithms where applicable, ensuring a high standard of data protection. All data in transit is securely transmitted using TLS 1.2 or higher, safeguarding against interception and unauthorized access. The management of encryption keys adheres to best practices, with keys being securely handled through Oracle Cloud’s Key Management Service. Access to these encryption keys is strictly controlled, with permissions limited to authorized personnel only, demonstrating JASCI Software’s commitment to maintaining robust encryption and key management practices.

3.2.3.4 Risk Assessment

During the audit of JASCI Software's risk management practices, it was confirmed that a comprehensive risk assessment is conducted annually to identify potential security threats. All findings from the assessment are thoroughly documented, and mitigation plans are developed to address identified risks, ensuring proactive management of security vulnerabilities. The company utilizes Oracle Cloud’s vulnerability scanning tools to continuously monitor and identify vulnerabilities, with timely remediation efforts in place to mitigate any risks. Additionally, patch management processes are executed in accordance with industry best practices, further enhancing the security posture of JASCI Software’s cloud infrastructure. This demonstrates a strong commitment to maintaining a secure and resilient environment.

3.2.3.5 Network Security

During the audit of JASCI Software's Oracle Cloud environment, it was verified that Oracle Cloud security groups and firewalls are properly configured to restrict unauthorized access to cloud resources, ensuring only authorized users and systems can interact with critical assets. Additionally, Oracle Cloud's Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) services have been effectively implemented to detect and prevent unauthorized access attempts, enhancing the overall security posture. The use of network segmentation further strengthens security by isolating sensitive systems from less critical ones, thereby minimizing potential access points for attackers and limiting the scope of any potential security breaches. These measures reflect JASCI Software's strong focus on securing its cloud infrastructure**.**

3.3 Complementary User Entity Controls (CUECs)

Complementary User Entity Controls (CUECs) refer to specific controls that a **service organization** expects its **user entities (clients)** to implement in order to help ensure the overall effectiveness of the system's security, availability, processing integrity, confidentiality, and privacy. These controls are complementary because they work together with the service organization's controls to meet the control objectives stated in a SOC 2 Type 2 report.

2.1.2 Purpose and Use of CUECs:

The main use of CUECs is to establish a clear division of responsibility between the service organization and its clients. While the service organization (e.g., JASCI Software) implements controls to safeguard its system, certain security or operational responsibilities must be handled by the clients themselves. CUECs help clarify what the clients need to do on their end to ensure their data and operations are secure when using the service provider's system.

2.1.3 Example in Practice:

If JASCI Software provides a cloud service, they may implement encryption and firewalls as part of their controls. However, they expect their clients to manage their own user access to the platform through strong authentication controls. These client-side controls (CUECs) are necessary to complement the security measures taken by JASCI Software and ensure a complete and effective security framework.

Here are some examples of **Complementary User Entity Controls (CUECs)**, which are controls that a service organization expects its clients (user entities) to implement to complement the service organization's controls and help achieve control objectives:

A. Access Control Management

- **Client Responsibility**: The user entity is responsible for managing its users' access to the service system, ensuring that access rights are granted only to authorized individuals.
- **Example**: The client should implement strong password policies, enforce multi-factor authentication (MFA), and conduct regular reviews of user access privileges.

SECTION 4: INFORMATION PROVIDED BY THE SERVICE AUDITOR: TEST OF CONTROLS

4.4 Testing Procedures Performed by Independent Service Auditor

In addition to the tests listed below for each control specified by JASCI Software, ascertained through inquiry with management and the controlling owner that each control activity listed below operated as described throughout the period.

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
Security Criteria			
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**		
1.1.1	The Company should require a mission and vision statement.	During the audit of JASCI Software, it was observed that the organization has effectively maintained its mission and vision statements, which are prominently posted on its official website.	No Exceptions Noted
1.1.2	Does the Company implement a whistle-blower program to identify financial irregularities, unethical practices and frauds?	During the audit of JASCI Software, it was observed that the company has established and maintained a well-defined whistle-blower policy. This policy effectively facilitates the identification and reporting of financial irregularities, unethical practices, and fraud.	No Exceptions Noted
1.1.3	The Company should approve code of Conduct that is applied across the entity. The Code of Conduct should outline strict disciplinary consequences for violation of code of conduct	During the audit of JASCI Software, it was observed that the company has maintained a well-defined code of conduct policy, which has been formally approved. This policy outlines the ethical standards and expectations for employee behavior, fostering a culture of integrity and professionalism within the organization.	No Exceptions Noted
1.1.4	All new employees are required Induction training and their joining/appointment letter in the Code of Conduct is also included. New employees should sign off that they have read this document. Existing employees, on an annual basis, must undergo refresher training on Company's policies on code of conduct.	During the audit of JASCI Software, it was observed that the company provides comprehensive induction training to all new employees. This training is designed to equip newcomers with essential knowledge about the organization’s policies, procedures, and culture, thereby facilitating a smooth integration into the workplace.	No Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
1.1.5	Performance appraisals should be performed at least annually.	JASCI Software has demonstrated compliance with employee performance management practices by providing documented evidence of performance appraisal forms. Additionally, the company conducts performance appraisals on an annual basis, ensuring a structured approach to evaluating employee performance and supporting continuous improvement	No Exceptions Noted
1.1.6	Vendor agreements, including any security, availability, and confidentiality commitments, are required to be reviewed by appropriate Entity management during the procurement process.	During the audit, it was observed that JASCI Software has maintained vendor agreements, demonstrating proper documentation and management of third-party relationships in compliance with organizational policies.	No Exceptions Noted
1.1.7	The entity must have a code of conduct within the Employee Handbook that establishes standards and guidelines for personnel ethical behavior.	During the audit of JASCI Software, it was observed that the company has maintained a well-defined code of conduct policy, which has been formally approved. This policy outlines the ethical standards and expectations for employee behavior, fostering a culture of integrity and professionalism within the organization.	No Exceptions Noted
1.1.8	NDA Should be a part of Code of Conduct and Data Protection Policy which all the new joiners required to sign upon joining.	During the audit of JASCI Software, it was observed that the company has maintained a well-defined code of conduct policy, which has been formally approved. This policy outlines the ethical standards and expectations for employee behavior, fostering a culture of integrity and professionalism within the organization.	No Exceptions Noted
1.1.9	As part of employee orientation, new hires are required to acknowledge their understanding and acceptance of all policies and Procedures which includes Acceptable Use Policy (AUP).	During the audit, it was observed that JASCI Software has maintained an Acceptable Usage Policy, ensuring clear guidelines for the proper and secure use of organizational resources by employees.	No Exceptions Noted
1.1.10	Agreements must be established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties and subcontractors.	During the audit, it was observed that JASCI Software has maintained vendor agreements, demonstrating proper documentation and management of third-party relationships in compliance with organizational policies.	No Exceptions Noted
1.1.11	Customer must provide their issues, complaints or feedback through Tickets	During the audit, it was observed that JASCI Software utilizes a ticketing system for managing complaints, ensuring efficient tracking, resolution, and documentation of issues raised by employees or stakeholders.	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.**		
1.2.1	The CISO-led Management Review Meetings should be conducted annually to address the security level, technological advancements, changes, incident occurrences, and security initiatives	During the audit of JASCI Software, it was observed that the company conducts management review meetings weekly to assess various aspects of its security framework. These meetings address the current security levels, technological advancements, changes in the operational environment, incident occurrences, and ongoing security initiatives.	No Exceptions Noted
1.2.2	The boot camp meetings required to take place every two weeks, addressing both business and operational matters	During the audit of JASCI Software, it was observed that the company conducts management review meetings weekly to assess various aspects of its security framework. These meetings address the current security levels, technological advancements, changes in the operational environment, incident occurrences, and ongoing security initiatives.	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.**		
1.3.1	Organization charts are required that depicts authority, reporting lines and responsibilities for management of its information systems.	During the audit, it was observed that JASCI Software does not have a management-approved organizational chart, which may lead to a lack of clarity in roles, responsibilities, and reporting structures within the organization. **Mitigation:** It is recommended that JASCI Software create and implement a formal organizational chart that is approved by management. This chart should clearly define roles, responsibilities, and reporting lines, ensuring effective communication and accountability. Regular reviews and updates should be conducted to reflect any organizational changes.	Exceptions Noted
1.3.2	Company must have Information security related policies and procedures that describes information security processes, practices and organization.	During the audit of JASCI Software, it was observed that the company has maintained well-defined information security-related policies and procedures. These documents comprehensively describe the organization's information security processes, practices, and governance structure.	No Exceptions Noted
1.3.3	Information Security Policy & Procedures related to HR policies must be reviewed and approved by the Management at least annually.	During the audit of JASCI Software, it was observed that the company has maintained well-defined information security-related policies and procedures. These documents comprehensively describe the organization's information security processes, practices, and governance structure.	No Exceptions Noted
1.3.4	The responsibility of managing Information Security should be assigned to CISO. Allocation of information security responsibility must be documented in Rolesand responsibilities.	During the audit, it was observed that JASCI Software has maintained a RACI matrix, ensuring clear assignment of roles and responsibilities across various processes and activities within the organization.	No Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**		
1.4.1	The company has documented HR Policies and procedures including recruitment, trainingand exit procedures.	During the audit of JASCI Software, it was observed that the company has maintained a well-defined human resource policy, which is formally approved and reviewed annually. This policy outlines the organization's approach to managing its workforce, including recruitment, training, performance management, and employee relations.	No Exceptions Noted
1.4.2	Job requirements must be documented in the job descriptions, and candidates' abilities to meet these requirementsare evaluated as part of the hiring and transfer process.	During the audit of JASCI Software, it was observed that the company has documented job descriptions for all positions within the organization. These job descriptions clearly outline the roles, responsibilities, and expectations associated with each position, ensuring that employees understand their duties and the skills required.	No Exceptions Noted
1.4.3	New employees must sign offer letter as their agreement and acceptance of broad terms of employment including a brief description of position and other terms.	During the audit, it was observed that JASCI Software provided the signed employment agreements for employees, demonstrating their adherence to organizational policies and confirming that all personnel are formally engaged under documented terms and conditions.	No Exceptions Noted
1.4.4	Management must evaluate the need for additional resources in order to achieve business objectives as part of its periodic managementmeetings	During the audit of JASCI Software, it was observed that the company conducts management review meetings weekly to assess various aspects of its security framework. These meetings address the current security levels, technological advancements, changes in the operational environment, incident occurrences, and ongoing security initiatives.	No Exceptions Noted
1.4.5	Internal HR Reference checks must be conducted by HR team or the hiring manager through document verification and references check with the former colleagues or managers provided in the resume	During the audit, it was observed that JASCI Software has maintained a reference check process, demonstrating due diligence in verifying candidate credentials during the hiring process.	No Exceptions Noted
1.4.6	Background verification checks are required to be carried out for experienced new hiresby the internal HR team. This includes education qualification verificationand employment verification.	During the audit of JASCI Software, it was observed that the company conducts background checks on prospective employees as part of its hiring process. This practice demonstrates JASCI Software's commitment to ensuring a safe and secure work environment by verifying the qualifications, integrity, and reliability of new hires.	No Exceptions Noted

1.4.7	Does company have any contract employees on existing projects	Not Applicable	Not Applicable
1.4.8	Company must have Information security related policies and procedures that describes information security processes, practices and organization.	During the audit of JASCI Software, it was observed that the company has maintained well-defined information security-related policies and procedures. These documents comprehensively describe the organization's information security processes, practices, and governance structure.	No Exceptions Noted
1.4.9	Newly hired personnel must be provided sufficient training before they assumethe responsibilities of their new position	During the audit of JASCI Software, it was observed that the company provides sufficient training to employees before they assume the responsibilities of their new positions. This training ensures that employees are adequately prepared and equipped with the necessary knowledge and skills to perform effectively in their roles.	No Exceptions Noted
1.4.10	The induction training given by HR must include information security training. In this training the HR, physical access and security policies are explained.	During the audit, it was observed that JASCI Software does not provide induction training to employees, which may result in a lack of awareness regarding company policies, processes, and roles, potentially affecting overall productivity and compliance. **Mitigation:** It is recommended that JASCI Software implement a formal induction training program for all new employees. This program should cover company policies, processes, security practices, and role-specific responsibilities.	Exceptions Noted
1.4.11	An awareness refresher training must be provided to all employees. It should be conducted quarterly and ensured that all the employees are covered atleast once a year.	During the audit of JASCI Software, it was observed that the company provides awareness refresher training to all employees.	No Exceptions Noted
1.4.12	Training calendars should be maintained by HR team. HR team circulates an emailed to all the employees informing them about the trainingsincluding ISMS awareness that are scheduled for the particular month	During the audit of JASCI Software, it was observed that the organization does not conduct an annual training program for all employees. However, the company ensures that each individual is specifically trained and qualified for their respective departmental roles.	No Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**		

1.5.1	Roles and responsibilities must be defined in written job descriptions and communicated to employees and theirmanagers	During the audit of JASCI Software, it was observed that the roles and responsibilities of employees are clearly defined in written job descriptions, which are effectively communicated to the staff. This practice ensures that employees understand their specific duties and expectations within the organization.	No Exceptions Noted
1.5.2	Is there a practice in place for entity management to review job descriptions on an annual basis as part of the performance appraisal process?	JASCI Software has demonstrated compliance with employee performance management practices by providing documented evidence of performance appraisal forms. Additionally, the company conducts performance appraisals on an annual basis, ensuring a structured approach to evaluating employee performance and supporting continuous improvement	No Exceptions Noted
1.5.3	Code of conduct is required to be uploaded on the website reviewed and updated as and when required	During the audit of JASCI Software, it was observed that the company's Code of Conduct is prominently uploaded on its official website.	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.**		
Ref No	**Controls Implemented by Entity**	**Test Procedures**	**Test Results**
2.1.1	Internal audits are required to be performed, results are communicated and corrective actions Monitored.	During the audit, it was observed that JASCI Software provided an internal audit report; however, the report does not meet standard requirements, which may impact the effectiveness of audit processes and compliance assurance. **Mitigation:** It is recommended that JASCI Software review and align its internal audit reporting process with standard requirements, such as including detailed findings, root cause analyses, risk assessments, and corrective action plans.	Exceptions Noted
2.1.2	A meeting is required to carry out Quarterly to hold department discussion and status updates	During the audit of JASCI Software, it was observed that the company conducts management review meetings weekly to assess various aspects of its security framework. These meetings address the current security levels, technological advancements, changes in the operational environment, incident occurrences, and ongoing security initiatives.	No Exceptions Noted

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.		
2.2.1	System boundaries in terms of logical and physical boundaries must be documented. Network diagrams should be inplace. System Boundaries must be shared with the customers when it is required.	During the audit, it was observed that JASCI Software has maintained an Information Security Policy, demonstrating its commitment to safeguarding information assets and ensuring compliance with security standards.	No Exceptions Noted
2.2.2	Customer responsibilities and appropriate system descriptions are required to be provided in client contracts.	During the audit of JASCI Software, it was observed that customer responsibilities and detailed system descriptions are clearly provided in client contracts. This practice ensures that both parties have a mutual understanding of their obligations and the services being rendered.	No Exceptions Noted
2.2.3	Are the Security policies communicated to employees.	During the audit, it was observed that JASCI Software has maintained Information Security Policies; however, these policies are not effectively communicated to employees, which may lead to a lack of awareness and adherence to security practices. **Mitigation:** It is recommended that JASCI Software establish a formal process to communicate Information Security Policies to all employees. This can include training sessions, awareness programs, and accessible policy repositories.	Exceptions Noted
2.2.4	Are the organizational wide incident management process in place	During the audit, it was observed that JASCI Software has maintained an Incident Management Procedure; however, the procedure lacks document control and version history, which may lead to difficulties in tracking changes, updates, and ensuring that employees are working with the most current version. **Mitigation:** It is recommended that JASCI Software implement a document control system for the Incident Management Procedure, including version history, approval dates, and clear tracking of revisions.	Exceptions Noted
2.2.5	Has the entity effectively communicated its commitment to security as a top priority for its customers through contracts and website pages	During the audit of JASCI Software, it was observed that the company effectively communicates its commitment to security as a top priority for its customers through various channels, including contracts and dedicated pages on its website. This clear communication reinforces the organization's dedication to safeguarding customer information and maintaining high security standards.	No Exceptions Noted

2.2.6	Is there a process in place to ensure that all system changes affecting both internal and external users are communicated in a timely manner	During the audit of JASCI Software, it was observed that the company has maintained a comprehensive change management policy. This policy outlines the processes for planning, approving, and implementing changes within the organization, ensuring that all changes are managed effectively to minimize disruption and maintain operational integrity.	No Exceptions Noted
2.2.7	Is external client communication consistently conducted in a timely manner by the Project Manager or IT Head using a standard client-specific escalation matrix	During the audit, it was observed that JASCI Software has maintained a Communication Policy, ensuring clear and consistent communication practices within the organization and with external stakeholders.	No Exceptions Noted
2.2.8	Banners must be provided on client facingapplications for communicating changes or downtime such as maintenance window	During the audit, it was observed that JASCI Software communicates changes or downtime, such as maintenance windows, to relevant stakeholders in a timely and effective manner, ensuring minimal disruption to operations.	No Exceptions Noted
2.2.9	CISO is responsible for decisions Regarding changes in confidentiality practices and commitments. Operations team must communicate these changes to the customers.	During the audit of JASCI Software, it was observed that the company actively communicates updates and decisions regarding changes in confidentiality practices and commitments to its customers. This approach ensures that clients are kept informed of any alterations that may impact the handling of their sensitive information.	No Exceptions Noted
2.2.10	Is it the practice for new employees hired at senior levels to communicate with stakeholders through email, facilitated by the HR department	During the audit, it was observed that senior-level new hires at JASCI Software directly email or communicate with stakeholders, ensuring clear and efficient engagement from the outset of their roles.	No Exceptions Noted
Ref No	**Controls Implemented by Entity**	**Test Procedures**	**Test Results**
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**		
2.3.1	Are the company's commitments regarding system security, availability, and confidentiality required to be included in client contracts or Statements of Work (SOW), or are there alternative methods for conveying these commitments	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
2.3.2	Are Security policies published on company website or any intranet portal?	During the audit of JASCI Software, it was observed that the company published and communicated all relevant policies to its employees. This practice ensures that all staff members are aware of the policies that	No Exceptions Noted

		govern their roles and responsibilities, promoting transparency and compliance within the organization.	
2.3.3	Does the induction training provided by HR include information security training, which covers explanations of HR processes, physical access procedures, and security policies	During the audit, it was observed that JASCI Software does not provide induction training to employees, which may result in a lack of awareness regarding company policies, processes, and roles, potentially affecting overall productivity and compliance. **Mitigation:** It is recommended that JASCI Software implement a formal induction training program for all new employees. This program should cover company policies, processes, security practices, and role-specific responsibilities.	Exceptions Noted
2.3.4	Are customer responsibilities described in client contracts, Master Service Agreements (MSAs), or Service Level Agreements (SLAs)	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
2.3.5	Users should be informed of the process for reporting complaints and security breaches during induction Security Training.	During the audit of JASCI Software, it was observed that users are informed of the processes for reporting complaints and security breaches during their induction security training. This training ensures that all employees understand the procedures and channels available for raising concerns, thereby promoting a proactive approach to security and accountability.	No Exceptions Noted
2.3.6	Is it possible for customers to submit their issues, complaints, or feedback via email to the Business Heads, while employees are allowed to raise their complaints and grievances with the HR department	During the audit, it was observed that employees at JASCI Software are able to submit their complaints via email, ensuring a clear and accessible channel for addressing concerns within the organization.	No Exceptions Noted
2.3.7	A client escalation matrix must be in place to ensure that communication channels for external users are available.	During the audit of JASCI Software, it was observed that the company has maintained a well-defined escalation matrix. This matrix clearly outlines the procedures for escalating issues and incidents within the organization, ensuring timely resolution and effective communication at all levels.	No Exceptions Noted
2.3.8	are the Whistle blower channels be available for external parties	During the audit of JASCI Software, it was observed that the company has maintained a well-defined whistle-blower policy. This policy provides a secure and confidential channel for employees to report any concerns related to unethical practices,	No Exceptions Noted

		financial irregularities, or misconduct without fear of retaliation.	
2.3.9	CISO is responsible for decisions regarding changes in confidentiality practices and commitments. Operations team should communicate these changes to the customers	During the audit of JASCI Software, it was observed that the company conducts management review meetings weekly to assess various aspects of its security framework. These meetings address the current security levels, technological advancements, changes in the operational environment, incident occurrences, and ongoing security initiatives.	No Exceptions Noted
2.3.10	Changes to system boundaries, network systems should be communicated to clients, if it impactstheir operations	During the audit, it was observed that JASCI Software has maintained a Change Management Policy, ensuring structured and controlled processes for implementing changes to systems and services, thereby minimizing risks and maintaining operational stability.	No Exceptions Noted
2.3.11	Incidents impacting external users should be communicated to them through emails along with root cause analysis,if required.	Not Appliacble	Not Appliacble
Ref No	**Controls Implemented by Entity**	**Test Procedures**	**Test Results**
	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.**		
3.1.1	Management must establish a process to periodically review and update entity-wide strategic plans and objectives.	During the audit, it was observed that JASCI Software has maintained a Strategic Planning Policy, ensuring a structured approach to setting and achieving organizational goals, aligning resources, and supporting long-term business objectives.	No Exceptions Noted
3.1.2	Risk Assessment Scales(Risk Rating scales) are required to be defined to evaluate and assessthe significance of Risk. Thisis part of the Risk Management Framework.	During the audit of JASCI Software, it was observed that the company has maintained a well-defined risk management policy.	No Exceptions Noted
3.1.3	Management must have a business planning Process in place that examines existing objectives and establishes new objectives when necessary.	During the audit of JASCI Software, it was observed that the company has maintained a well-defined information security policy. This policy outlines the principles and practices that govern the protection of sensitive information, ensuring compliance with relevant regulations and standards.	No Exceptions Noted

3.1.4	Policies and procedures related to risk Management should be developed, implemented, and communicated to personnel.	During the audit of JASCI Software, it was observed that the company has maintained a well-defined risk management policy.	No Exceptions Noted
3.1.5	Management must evaluate the need for additional resources in order to achieve business objectives as part of its periodic management meetings	During the audit of JASCI Software, it was observed that management evaluates the need for additional resources to achieve business objectives as part of its periodic management meetings. This practice ensures that the organization remains agile and responsive to its operational requirements, facilitating informed decision-making regarding resource allocation.	No Exceptions Noted
CC3.2	**COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.**		
Ref No	**Controls Implemented by Entity**	**Test Procedures**	**Test Results**
3.2.1	Policies and procedures related to risk Management should be developed, implemented, and communicated to personnel.	During the audit, it was observed that JASCI Software has maintained a Risk Assessment Policy, ensuring a systematic approach to identifying, evaluating, and managing risks to protect the organization's assets and achieve its objectives.	No Exceptions Noted
3.2.2	Is there a practice in place where a risk assessment is conducted annually or whenever there are changes in the security posture, during which threats to security are identified and their associated risks are formally assessed	During the audit, it was observed that JASCI Software has maintained a Risk Assessment Policy, ensuring a systematic approach to identifying, evaluating, and managing risks to protect the organization's assets and achieve its objectives.	No Exceptions Noted
3.2.3	The Risk and Compliance team should monitor the environment of internal control and identifies significant changes that have occurred.	During the audit, it was observed that JASCI Software provided an internal audit report; however, the report does not meet standard requirements, which may impact the effectiveness of audit processes and compliance assurance. **Mitigation:** It is recommended that JASCI Software review and align its internal audit reporting process with standard requirements, such as including detailed findings, root cause analyses, risk assessments, and corrective action plans.	Exceptions Noted
3.2.4	Identified risks are required to be rated and get prioritized based on their likelihood, impact, detection and the existing control measures.	During the audit, it was observed that JASCI Software has maintained a Risk Assessment Policy, ensuring a systematic approach to identifying, evaluating, and managing risks to protect the organization's assets and achieve its objectives.	No Exceptions Noted

3.2.5	All information assets should be identified in an asset inventory	During the audit, it was observed that JASCI Software provided an asset inventory; however, it does not meet standard requirements, lacking essential details such as asset classification, ownership, and lifecycle information, which may affect the organization's ability to manage and secure its assets effectively. **Mitigation:** It is recommended that JASCI Software update its asset inventory to comply with standard requirements, including comprehensive details such as asset classification, ownership, location, and lifecycle stages.	Exceptions Noted
3.2.6	Monitoring tools must be implemented to detect control issues	During the audit, it was observed that JASCI Software has implemented monitoring tools, enabling proactive tracking and management of system performance, security, and compliance to ensure operational efficiency and risk mitigation.	No Exceptions Noted
3.2.7	Vulnerability Assessment should be done internally by the team every six months. Internal Penetration tests are required to be done by team on a yearly basis.	During the audit, it was observed that JASCI Software provided a VAPT (Vulnerability Assessment and Penetration Testing) report; however, the report does not meet standard requirements, lacking comprehensive details such as severity ratings, risk assessments, and recommended remediation steps for identified vulnerabilities. **Mitigation:** It is recommended that JASCI Software ensure the VAPT report includes all necessary details as per standard requirements, such as clear identification of vulnerabilities, severity ratings, risk assessments, and specific remediation actions.	Exceptions Noted
CC 3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**		
3.3.1	How the entity patch management run periodically to automatically update user systems.	During the audit, it was observed that JASCI Software has maintained a Patch Management process, ensuring that systems and software are regularly updated to address security vulnerabilities and improve overall system performance and stability.	No Exceptions Noted
3.3.2	List of all hardware must be maintained as Part of asset register	During the audit, it was observed that JASCI Software provided an asset register; however, it lacks formal approval, which may affect its credibility and alignment with company policies. **Mitigation:** It is recommended that JASCI Software implement a formal approval process for the asset register. This should include approval	Exceptions Noted

		by management or designated personnel to ensure the register is accurate, complete, and aligns with organizational policies.	
3.3.3	Company must define a formal risk Management process for evaluating risks based on identifiedvulnerabilities,threats , asset value and mitigating controls	During the audit of JASCI Software, it was observed that the company has maintained a well-defined risk management policy.	No Exceptions Noted
3.3.4	Management should evaluate the effectiveness of controls and mitigation strategies in meeting identified risks and recommends changes based on its evaluation	During the audit, it was observed that JASCI Software provided an internal audit report; however, the report does not meet standard requirements, which may impact the effectiveness of audit processes and compliance assurance. **Mitigation:** It is recommended that JASCI Software review and align its internal audit reporting process with standard requirements, such as including detailed findings, root cause analyses, risk assessments, and corrective action plans.	No Exceptions Noted
CC 3.4	**COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**		
3.4.1	Is it a standard practice to conduct a risk assessment whenever new products or services are introduced or when there are changes to the business model for these new offerings	During the audit, it was observed that JASCI Software provided a risk register; however, it lacks formal approval and document control, which may impact its effectiveness in managing and mitigating risks across the organization. **Mitigation:** It is recommended that JASCI Software implement a formal approval process for the risk register, ensuring it is reviewed and approved by management or designated personnel	Exceptions Noted
3.4.2	Are the Emerging technology and system changes considered when performing risk assessment	During the audit, it was observed that JASCI Software provided a risk register; however, it lacks formal approval and document control, which may impact its effectiveness in managing and mitigating risks across the organization. **Mitigation:** It is recommended that JASCI Software implement a formal approval process for the risk register, ensuring it is reviewed and approved by management or designated personnel	Exceptions Noted

3.4.3	Vendor agreements, including any Security, availability and confidentiality commitments, are required to be reviewed by appropriate senior management during the procurement process.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
Ref No	**Controls Implemented by Entity**	**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.**		
4.1.1	The internal audit function conducts System security reviews quarterly. Results and recommendations for improvement are required to be reported to management.	During the audit, it was observed that JASCI Software provided an internal audit report; however, the report does not meet standard requirements, which may impact the effectiveness of audit processes and compliance assurance. **Mitigation:** It is recommended that JASCI Software review and align its internal audit reporting process with standard requirements, such as including detailed findings, root cause analyses, risk assessments, and corrective action plans.	Exceptions Noted
4.1.2	Are the Internal audit team staffed with Competent professionals with technical expertise.	During the audit, it was observed that JASCI Software provided an internal audit report; however, the report does not meet standard requirements, which may impact the effectiveness of audit processes and compliance assurance. **Mitigation:** It is recommended that JASCI Software review and align its internal audit reporting process with standard requirements, such as including detailed findings, root cause analyses, risk assessments, and corrective action plans.	No Exceptions Noted
4.1.3	Is there an established audit calendar that covers all locations and business units, with the frequency of audits being adjusted to address high risks	During the audit of JASCI Software, it was observed that the organization does not conduct an annual training program for all employees. However, the company ensures that each individual is specifically trained and qualified for their respective departmental roles.	No Exceptions Noted
4.1.4	IT system access is required to be reviewed on amonthly basis.	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities,	No Exceptions Noted

		thereby enhancing security and compliance.	
CC 4.2	**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.**		
4.2.1	Is the firewall configured to log events, and are these logs reviewed on a periodic basis	During the audit, it was observed that JASCI Software has maintained a Firewall Configuration Policy, ensuring that firewalls are properly configured and managed to protect the organization's network from unauthorized access and security threats.	No Exceptions Noted
4.2.1	All internal audit issues must be tracked until closure to ensure that these are closed.	During the audit, it was observed that JASCI Software provided an internal audit report; however, the report does not meet standard requirements, which may impact the effectiveness of audit processes and compliance assurance. **Mitigation:** It is recommended that JASCI Software review and align its internal audit reporting process with standard requirements, such as including detailed findings, root cause analyses, risk assessments, and corrective action plans.	Exceptions Noted
Ref No	**Controls Implemented by Entity**	**Test Procedures**	**Test Results**
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.**		
5.1.1	Vulnerability assessment & penetration tests must be performed annually by a third party.	During the audit, it was observed that JASCI Software provided a VAPT (Vulnerability Assessment and Penetration Testing) report; however, the report does not meet standard requirements, lacking comprehensive details such as severity ratings, risk assessments, and recommended remediation steps for identified vulnerabilities. **Mitigation:** It is recommended that JASCI Software ensure the VAPT report includes all necessary details as per standard requirements, such as clear identification of vulnerabilities, severity ratings, risk assessments, and specific remediation actions.	Exceptions Noted
5.1.2	IT system access is required to be reviewed on a Quarterly basis.	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted

5.1.3	All major business functions are required to covered in the internal audit process.	During the audit of JASCI Software, it was observed that the organization does not conduct an annual training program for all employees. However, the company ensures that each individual is specifically trained and qualified for their respective departmental roles.	No Exceptions Noted
5.1.4	As a small firm, there is no adequate segregation of duties. However, compensating monitoring controls must be in place to ensure any internal control failures are detected.	During the audit, it was observed that JASCI Software utilizes New Relic for server and database monitoring, ensuring real-time performance tracking and proactive issue management to maintain system reliability.	No Exceptions Noted
CC 5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**		
5.2.1	Policies and proceduresrelated to risk Management are required to be developed, implemented, and communicated to personnel.	During the audit, it was observed that JASCI Software has maintained a Risk Assessment Policy, ensuring a systematic approach to identifying, evaluating, and managing risks to protect the organization's assets and achieve its objectives.	No Exceptions Noted
CC 5.3	**COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**		
5.3.1	The Company should have implemented major Policies and SOPs across business functions. Procedures must be documented using various formats, such as narratives, flowcharts, and control matrices	During the audit, it was observed that JASCI Software has maintained a list of policies.	No Exceptions Noted
5.3.2	Are all policies reviewed at least annually to ensure they remain current and aligned with the current business practices	Not Applicable	Not Applicable
5.3.3	Are significant policies and procedures accessible to all employees who need to refer to them	During the audit, it was observed that JASCI Software provided a user permission document, ensuring proper documentation of user access rights and permissions to maintain secure and controlled access to systems and resources.	No Exceptions Noted
5.3.4	Does the internal audit department assess the adequacy and relevance of policies and procedures	During the audit, it was observed that JASCI Software provided an internal audit report; however, the report does not meet standard requirements, which may impact the effectiveness of audit processes and compliance assurance. **Mitigation:** It is recommended that JASCI Software review and align its internal audit reporting process with standard requirements, such as including detailed findings, root cause analyses, risk assessments, and corrective action plans.	Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
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.**		
6.1.1	Company must have documented procedure for logical access controls	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted
6.1.2	Access should be granted on least privileges Basis as default and any additional access needs to be approved.	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted
6.1.3	Has the company established hardening standards for Windows Server, Linux Server, and Firewall configurations for its production infrastructure	During the audit, it was observed that JASCI Software has provided a hardening standard, ensuring that systems and applications are securely configured to minimize vulnerabilities and reduce the risk of unauthorized access or security breaches.	No Exceptions Noted
6.1.4	Are physical and logical diagrams of networking devices, such as routers, firewalls, switches, servers (including wireless components), documented for the office network	During the audit, it was observed that JASCI Software provided a network diagram; however, it does not contain version history, which may hinder the tracking of changes and updates to the network architecture over time. **Mitigation:** It is recommended that JASCI Software implement a version control process for the network diagram. This should include documenting version history, along with changes made and the date of updates.	Exceptions Noted
6.1.5	Company should not allow customers or external users to access its systems	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted
6.1.6	Is the infrastructure's components and software configured to utilize Windows security through group policies and Active Directory	During the audit, it was observed that JASCI Software has provided an Active Directory Policy, ensuring the proper management and security of user accounts, access rights, and resources within the organization's network infrastructure.	No Exceptions Noted
6.1.7	Is access to application instances hosted for clients restricted to the IT support team and select client project team members who require access? Additionally, does the IT support team have administrative rights and the capability to add additional users from the client's entity to	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted

	these instances based on business needs		
6.1.8	The Company must have a VPN/remote working policy that requires that external access is granted on a need Basis.	During the audit, it was observed that JASCI Software has provided a Remote Working Policy, ensuring that employees are guided on secure and effective practices while working remotely, in alignment with the organization's security and operational standards.	No Exceptions Noted
6.1.9	The IT department maintains an Up-to-date listing of all software.	During the audit, it was observed that JASCI Software has provided an up-to-date list of software, ensuring accurate documentation of all applications and tools in use, which supports effective asset management and security control.	No Exceptions Noted
6.1.10	All Assets must be assigned owners Who are responsible for evaluating access based on job roles? The owners define access rights when assets are acquired or changed.	During the audit, it was observed that JASCI Software has provided an asset register, ensuring proper documentation and tracking of all organizational assets, which supports effective asset management and security.	No Exceptions Noted
6.1.11	Is privileged access to sensitive resources restricted to defined user roles, with access to these roles requiring approval from management? Additionally, is privileged access authorized by the Chief Technology Officer (CTO) and periodically reviewed by the IT department	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted
6.1.12	Are the entity's systems configured to utilize Active Directory shared sign-on functionality	Not Applicable	Not Applicable
6.1.13	Account sharing must be prohibited Unless approved bymanagement.	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted
6.1.14	Do external users have access to the system only through remote methods such as VPN, secure sockets layer (SSL), or other encrypted communication systems	During the audit, it was observed that JASCI Software has provided a Remote Working Policy, ensuring that employees are guided on secure and effective practices while working remotely, in alignment with the organization's security and operational standards.	No Exceptions Noted
6.1.15	The following password parameters must be in place for active directory: 1. length of 8-characterlength 2. complexity is enabled 3. password expiresin 30 days 4. Password history is set at 5	During the audit, it was observed that JASCI Software provided evidence of password configuration settings, demonstrating the implementation of secure password policies to safeguard access to systems and protect sensitive information.	No Exceptions Noted

6.1.16	Is access to data restricted to authorized applications through domain policies via Active Directory? Is access to company systems granted only upon authorization, and are new employees provided with the principle of least privilege in their access permissions	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted
6.1.17	External access must be through firewall appliance that allows only the white listed IP addresses.	During the audit, it was observed that JASCI Software has maintained a Firewall Configuration Policy, ensuring that firewalls are properly configured and managed to protect the organization's network from unauthorized access and security threats.	No Exceptions Noted
6.1.18	Is all confidential data classified according to the data classification policy	During the audit, it was observed that JASCI Software has maintained a Data Classification Policy, ensuring that data is properly classified and protected according to its sensitivity and importance, in alignment with security and compliance requirements.	No Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
CC6.2	**Before 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.**		
6.2.1	Is it the practice that on an employee's day of joining, HR sends a mail to the IT helpdesk with the new joiner's details, and IT subsequently grants the necessary access as requested? Additionally, is the removal of employee user accounts from various applications and network systems done manually based on access revocation requests sent by the HR department as of the last date of employment	During the audit, it was observed that IP whitelist requests from employees at JASCI Software are submitted via Teams messages, providing a convenient and documented communication channel for handling such requests.	No Exceptions Noted
6.2.2	Is it the procedure that when an employee leaves the organization, the employee's manager initiates the 'Exit Process,' and HR informs the respective teams or IT team within 24 hours to deactivate or delete the user ID from the email system and all applications? Additionally, is an exit checklist employed to ensure compliance with termination procedures	During the audit, it was observed that JASCI Software has maintained an Exit Procedure, ensuring that proper protocols are followed when employees leave the organization, including the secure handling of company assets and access rights.	No Exceptions Noted
6.2.3	Privileged access to sensitive resources is required to restricted to defined user roles and access to these roles must be approved by Management. Privileged access must be authorized by CTO and reviewed by IT on a periodic basis.	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted

6.2.4	Company should not allow non-employees to accessits systems	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted
6.2.5	Company should not employ contractors in its offices.	Not Applicable	Not Applicable

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
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, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.**		
6.3.1	A role-based security process is required to setup in Active directory with groups and roles based on job requirements.	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted
6.3.2	Are the System access reviewed on a Quarterly basis.	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted
6.3.3	Company must not allow reactivation of ID belonging to an exited employee.	During the audit, it was observed that JASCI Software provided evidence of user access deactivation, demonstrating that appropriate measures are in place to promptly remove access for users who no longer require it, ensuring system security and compliance.	No Exceptions Noted
CC6.4	**The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.**		
6.4.1	Is access to all office premises restricted exclusively to authorized personnel	During the audit, it was observed that JASCI Software has maintained a Physical Security Policy, ensuring that adequate measures are in place to protect the organization's physical assets, facilities, and personnel	No Exceptions Noted

		from unauthorized access and security threats.	
6.4.2	Is physical access to office premises monitored through CCTV cameras installed at key points within the premises	Not Appliacble	Not Appliacble
6.4.3	All visitors must have to enter their details in the visitor register	During the audit, it was observed that JASCI Software has maintained a Visitor Policy, ensuring that appropriate controls are in place to manage and monitor visitor access to company premises, safeguarding physical security and confidentiality.	No Exceptions Noted
6.4.4	Is it a requirement for all visitors to enter their details in the visitor register	During the audit, it was observed that JASCI Software has maintained a Visitor Policy, ensuring that appropriate controls are in place to manage and monitor visitor access to company premises, safeguarding physical security and confidentiality.	No Exceptions Noted
6.4.5	Is it mandatory for all visitors to be accompanied by a company employee when they visit office facilities	During the audit, it was observed that JASCI Software has maintained a Visitor Policy, ensuring that appropriate controls are in place to manage and monitor visitor access to company premises, safeguarding physical security and confidentiality.	No Exceptions Noted
6.4.6	ID cards that include an employee picture must be worn at all times when accessing or leaving the facility.	During the audit, it was observed that JASCI Software has maintained a Physical Security Policy, ensuring that adequate measures are in place to protect the organization's physical assets, facilities, and personnel from unauthorized access and security threats.	No Exceptions Noted
6.4.7	Is there a standard procedure for the HR Department to set up physical access for new joiners after completing all HR formalities? Additionally, are ID cards issued to new joiners initially without access to sensitive areas	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted

6.4.8	Entry to the data center must be role based and controlled via dual authentication biometric & card access. Access to such restricted zone is required to be given against written request by the team leads	During the audit, it was observed that JASCI Software has maintained a Physical Security Policy, ensuring that adequate measures are in place to protect the organization's physical assets, facilities, and personnel from unauthorized access and security threats.	No Exceptions Noted
6.4.9	Periodic review of physical access to sensitive areas against active employee list should be carried out by IT.	During the audit, it was observed that JASCI Software has maintained a Physical Security Policy, ensuring that adequate measures are in place to protect the organization's physical assets, facilities, and personnel from unauthorized access and security threats.	No Exceptions Noted
6.4.10	Is it the practice for the HR team to send an exit email on the last day of employment, requesting the deactivation of physical access for terminated employees	During the audit, it was observed that JASCI Software provided evidence related to terminated employees, demonstrating proper documentation and adherence to employment termination processes.	No Exceptions Noted
6.4.11	Employees are required to return their ID cards on the lastday, and all ID badges are disabled.	During the audit, it was observed that JASCI Software provided evidence of terminated employees, demonstrating that proper procedures are followed to ensure the secure and compliant offboarding of employees, including the revocation of access and return of company assets.	No Exceptions Noted
6.4.12	The sharing of access badges and tailgating is prohibited by policy?.	During the audit, it was observed that JASCI Software has maintained a Physical Security Policy, ensuring that adequate measures are in place to protect the organization's physical assets, facilities, and personnel from unauthorized access and security threats.	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.**		
6.5.1	Is all media physically destroyed before disposal	During the audit, it was observed that JASCI Software has maintained a Data Disposal Policy, ensuring that data is securely and properly disposed of when no longer needed, in accordance with security standards and regulatory	No Exceptions Noted

		requirements.	
CC 6.6	**The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**		
6.6.1	Are external points of connectivity within the office network protected by a firewall	During the audit, it was observed that JASCI Software has maintained a Firewall Configuration Policy, ensuring that firewalls are properly configured and managed to protect the organization's network from unauthorized access and security threats.	No Exceptions Noted
6.6.2	Are incoming connections accepted only from whitelisted IPs in the firewall	During the audit, it was observed that JASCI Software has maintained a Firewall Configuration Policy, ensuring that firewalls are properly configured and managed to protect the organization's network from unauthorized access and security threats.	No Exceptions Noted
6.6.3	Access to modify firewall rules is required to be restricted by management.	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted
6.6.4	No confidential output should be printed internally in the office. No customer confidential data resides in office premises.	During the audit, it was observed that JASCI Software has maintained a Physical Security Policy, ensuring that adequate measures are in place to protect the organization's physical assets, facilities, and personnel from unauthorized access and security threats.	No Exceptions Noted
6.6.5	Logical access to Company systems is required to be restricted through active directory based domain policies.	During the audit, it was observed that JASCI Software has maintained an Access Control Policy, ensuring that access to sensitive information and systems is appropriately restricted based on roles and responsibilities, thereby enhancing security and compliance.	No Exceptions Noted

6.6.6	Data must be stored in encrypted format	During the audit, it was observed that JASCI Software has maintained an Encryption Policy, ensuring that sensitive data is protected through encryption both at rest and in transit, in alignment with industry best practices and security standards.	No Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
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.**		
6.7.1	Do the entity's policies prohibit the transmission of sensitive information over the Internet or other public networks	During the audit, it was observed that JASCI Software has maintained both an Information Security Policy and a Network Security Policy, ensuring comprehensive protection of organizational data and network infrastructure against security threats, in alignment with industry standards and best practices.	No Exceptions Noted
6.7.2	Are VPN connections to both corporate networks encrypted	During the audit, it was observed that JASCI Software has maintained an Encryption Policy, ensuring that sensitive data is protected through encryption both at rest and in transit, in alignment with industry best practices and security standards.	No Exceptions Noted
6.7.3	Use of removable media must be prohibited by policy except when authorized by management	During the audit, it was observed that JASCI Software has maintained a Removable Media Policy, ensuring the secure use, handling, and storage of removable media devices to protect sensitive data and prevent unauthorized access or data breaches.	No Exceptions Noted
6.7.4	Storage for laptops must be encrypted through bit locker encryption.	During the audit, it was observed that JASCI Software mandates all employees to enable BitLocker or equivalent encryption on their devices, ensuring that data stored on these laptops is securely encrypted and protected from unauthorized access.	No Exceptions Noted
CC 6.8	**The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.**		
6.8.1	Is Symantec antivirus software installed on workstations, laptops, and servers, providing features such as antivirus system scans, email scans, content filtering, and	During the audit, it was observed that JASCI Software has maintained an Antivirus Policy, ensuring that appropriate antivirus software is implemented and regularly updated	No Exceptions Noted

	endpoint protection	across the organization to protect systems from malware and security threats.	
6.8.2	"Are signature files for antivirus software updated on a daily basis, and does the antivirus console provide compliance reports regarding machines that have not been updated	During the audit, it was observed that JASCI Software has maintained an Antivirus Policy, ensuring that appropriate antivirus software is implemented and regularly updated across the organization to protect systems from malware and security threats.	No Exceptions Noted
6.8.3	The ability to install software on workstations and laptops is required to restricted to IT support personnel through domain policies.	During the audit, it was observed that JASCI Software provided evidence of the list of admin users, ensuring that administrative access is properly documented and managed to maintain control over critical systems and sensitive information.	No Exceptions Noted
6.8.4	Local admin access should be granted on a need based approval fromIT Infrastructure Head.	During the audit, it was observed that JASCI Software provided evidence of the access request form, ensuring that access to systems and resources is properly requested, reviewed, and authorized in accordance with security policies and procedures.	No Exceptions Noted
6.8.5	Any viruses discovered are required to reported to IT team either by the antivirus system or by the affected employees.	During the audit, it was observed that JASCI Software has maintained an Antivirus Policy, ensuring that appropriate antivirus software is implemented and regularly updated across the organization to protect systems from malware and security threats.	No Exceptions Noted
CC 7.1	**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.**		
7.1.1	Management has defined configuration standards and hardening standards.	During the audit, it was observed that JASCI Software has provided a hardening standard, ensuring that systems and applications are securely configured to minimize vulnerabilities and reduce the risk of unauthorized access or security breaches.	No Exceptions Noted
CC 7.2	**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.**		
7.2.1	Hardening Policy must be in place for hardening of IT infrastructure/desktops.	During the audit, it was observed that JASCI Software has provided a hardening standard, ensuring that systems and applications are securely configured to minimize vulnerabilities and reduce the risk of unauthorized access or security breaches.	No Exceptions Noted

7.2.2	Does the firewall protecting the corporate network send notifications of suspicious activity to the IT team, and are these alerts responded to promptly	During the audit, it was observed that JASCI Software has maintained a Firewall Configuration Policy, ensuring that firewalls are properly configured and managed to protect the organization's network from unauthorized access and security threats.	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.**		
7.3.1	Is there a formal, defined incident management process documented in the Security Incident Management Policy for evaluating reported events	During the audit, it was observed that JASCI Software has maintained an Incident Management Policy, ensuring that incidents are effectively identified, reported, and managed to minimize impact and ensure a timely and coordinated response to security events.	No Exceptions Noted
7.3.2	Incidents should be reported to the IT team. Forms should be maintained of incident.	Not Applicable	Not Applicable

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
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.**		
7.4.1	Are all security incidents be reviewed and monitored by the Management during Management Review Meetings. Corrective and preventive actions must be completed for incidents.	During the audit, it was observed that JASCI Software has maintained an Incident Management Policy, ensuring that incidents are effectively identified, reported, and managed to minimize impact and ensure a timely and coordinated response to security events.	No Exceptions Noted
7.4.2	Change management requests are required to open for events that require permanent fixes	During the audit, it was observed that JASCI Software has maintained a Change Management Policy, ensuring that all changes to systems, processes, and infrastructure are properly planned, tested, and approved to minimize risks and maintain operational integrity.	No Exceptions Noted
7.4.3	All incidents should be evaluated and necessary action taken to close the threat / vulnerability	During the audit, it was observed that JASCI Software provided evidence of the incident maintenance form, demonstrating that incidents are properly documented and tracked, ensuring an organized and effective response and resolution process.	No Exceptions Noted
7.4.4	Protocols for communicating security incidents and actions taken to affected parties are required to be developed and	Not Appliacble	Not Appliacble

	implemented to meet the entity's objectives.		
7.4.5	Reported incidents must be logged as tickets and include the following details Severity Data and Time of incident Details Status Root Cause (High, urgent severity incidents only)	During the audit, it was observed that JASCI Software has maintained an Incident Management Policy, ensuring that incidents are effectively identified, reported, and managed to minimize impact and ensure a timely and coordinated response to security events.	No Exceptions Noted
7.4.6	Quarterly, management reviews all incidents that occurred during the quarter.	During the audit, it was observed that JASCI Software has maintained an Incident Management Policy, ensuring that incidents are effectively identified, reported, and managed to minimize impact and ensure a timely and coordinated response to security events.	No Exceptions Noted
7.4.7	HR policies must include code of conduct and disciplinary policy for employee misconduct.	During the audit, it was observed that JASCI Software has maintained a Disciplinary Policy, ensuring that clear procedures are in place to address violations of company policies and maintain a fair and consistent approach to employee conduct and behavior.	No Exceptions Noted
CC7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**		
7.5.1	All incidents should be evaluated and necessary action taken to close the threat / vulnerability	During the audit, it was observed that JASCI Software has maintained an Incident Response Policy, ensuring that a structured and effective approach is in place to detect, respond to, and recover from security incidents, minimizing potential impact on the organization.	No Exceptions Noted
7.5.2	Root cause analysis performing for high & urgent incidents.	During the audit, it was observed that JASCI Software has maintained an Incident Response Policy, ensuring that a structured and effective approach is in place to detect, respond to, and recover from security incidents, minimizing potential impact on the organization.	No Exceptions Noted
7.5.3	The entity implements incident (BCP) recovery plan required to be tested on anannual basis	During the audit, it was observed that JASCI Software has maintained a Business Continuity Plan, ensuring that strategies and procedures are in place to maintain critical business operations and recover swiftly in the event of a disruption or emergency.	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.**		
8.1.1	Is it a requirement that all change requests undergo peer review by another programmer	During the audit, it was observed that JASCI Software has maintained a Change Management Policy, ensuring that all	No Exceptions Noted

	to ensure consistency	changes to systems, applications, and infrastructure are systematically planned, assessed, approved, and implemented to minimize disruptions and maintain operational integrity.	
8.1.2	Software code must be maintained in GIT.	During the audit, it was observed that JASCI Software provided evidence of the software code location, demonstrating that the company maintains secure and organized storage for its software code to ensure proper access control and protection of intellectual property.	No Exceptions Noted
8.1.3	Are software development changes tested through both unit testing and QA testing, with each of these activities being documented and monitored in change requests? Additionally, are test plans utilized by the QA team for testing	During the audit, it was observed that JASCI Software provided evidence of the Change Request Form, demonstrating that all changes are formally requested, documented, and reviewed in accordance with the company's change management process.	No Exceptions Noted
8.1.4	Is there a formal release process in place for releasing builds, where release notes specify what is included in the release, and the testing team conducts comprehensive testing of the release	During the audit, it was observed that JASCI Software has maintained a Code Release Document, ensuring that software releases are properly documented, approved, and tracked to maintain control and integrity throughout the development and deployment process.	No Exceptions Noted
8.1.5	All change requests required to submitted with implementation and backup plans	During the audit, it was observed that JASCI Software provided evidence of the Change Request Form, demonstrating that all changes are formally requested, documented, and reviewed in accordance with the company's change management process.	No Exceptions Noted
8.1.6	The change management process must have defined roles and assignments thereby providing segregation of roles in the change management process	During the audit, it was observed that JASCI Software has maintained a Change Management Policy, ensuring that all changes to systems, applications, and infrastructure are systematically planned, assessed, approved, and implemented to minimize disruptions and maintain operational integrity.	No Exceptions Noted
8.1.7	Entity have define its change management and approval processes in its information security policies	During the audit, it was observed that JASCI Software has maintained a Change Management Policy, ensuring that all changes to systems, applications, and infrastructure are systematically planned, assessed, approved, and implemented to minimize disruptions and maintain operational integrity.	No Exceptions Noted
8.1.8	For high, urgent severity incidents, change requests must be created.	During the audit, it was observed that JASCI Software has maintained both a Change Management Policy and an Incident Management Policy, ensuring that changes to systems and processes are systematically	No Exceptions Noted

		controlled, while security incidents are promptly detected, reported, and managed to minimize risk and operational disruption.	
8.1.9	Is there a process in place to manage mandatory changes, and are these changes, due to their urgent nature, allowed to be performed without prior review	During the audit, it was observed that JASCI Software has maintained a Change Management Policy, ensuring that all changes to systems, applications, and infrastructure are systematically planned, assessed, approved, and implemented to minimize disruptions and maintain operational integrity.	No Exceptions Noted
8.1.10	Data for testing must be crested manually before being used in testing	During the audit, it was observed that JASCI Software has maintained a Code Release Document, ensuring that software releases are properly documented, approved, and tracked to maintain control and integrity throughout the development and deployment process.	No Exceptions Noted
Ref No	**Controls Implemented by Entity**	**Test Procedures**	**Test Results**
Risk Mitigation			
CC9.1	**The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**		
9.1.1	Does the entity have a documented Business Continuity Plan (BCP) and Disaster Recovery (DR) guideline that can be used in the event of an incident requiring systems infrastructure recovery	During the audit, it was observed that JASCI Software has maintained a Business Continuity Plan, ensuring that strategies and procedures are in place to maintain critical business operations and recover swiftly in the event of a disruption or emergency.	No Exceptions Noted
9.2.2	Are business continuity and disaster recovery plans, including the restoration of backups, tested on an annual basis	During the audit, it was observed that JASCI Software has maintained a Business Continuity Plan, ensuring that strategies and procedures are in place to maintain critical business operations and recover swiftly in the event of a disruption or emergency.	No Exceptions Noted
Ref No	**Controls Implemented by Entity**	**Test Procedures**	**Test Results**
CC9.2	**The entity assesses and manages risks associated with vendors and business partners.**		
9.2.1	New Third-Party Service Providers are required to be selected based on a Vendor Selection Process. Security risk assessment should be key part of the vendor selection process. Company requires all key subservices to be compliant with security certifications and attestationssuch as ISO 27001, SOC1 or SOC2	Not Applicable	Not Applicable

9.2.2	All customer & vendor contracts must have terms related to confidentiality.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
9.2.3	There should be no information sharing with vendors or any third party	During the audit, it was observed that JASCI Software has maintained Non-Disclosure Agreements (NDAs) with clients, ensuring that confidential and sensitive information shared during the course of business is protected and handled in accordance with legal and regulatory requirements.	No Exceptions Noted
9.2.4	Is it a standard practice for all employees to sign a confidentiality agreement upon joining, and are Non-Disclosure Agreements (NDAs) signed with third parties as needed	During the audit, it was observed that JASCI Software has maintained Non-Disclosure Agreements (NDAs) with clients, ensuring that confidential and sensitive information shared during the course of business is protected and handled in accordance with legal and regulatory requirements.	No Exceptions Noted

Ref No	Controls Implemented by Entity	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.**		
1.1.1	Does the entity regularly monitor system processing capacity and usage and take corrective actions to address any changes or issues	During the audit of JASCI Software, it was observed that the company provided a comprehensive capacity monitoring report. This report reflects the organization's commitment to proactively managing and monitoring system capacity to ensure optimal performance and scalability, aligning with operational and business requirements.	No Exceptions Noted
1.1.2	Have critical infrastructure components undergone a review for criticality classification and the assignment of a minimum level of redundancy	Not Applicable	Not Applicable

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
A1.2	**The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.**		
1.2.1	Environmental controls (fire extinguishers, fire sprinklers and smoke detectors) should be installed to protect perimeter area. CCTV are required to be installed at key points for surveillance	During the audit of JASCI Software, it was observed that the company has established and maintained a comprehensive Physical Security Policy. This policy outlines the measures and controls in place to safeguard the organization's physical assets, infrastructure, and personnel, demonstrating JASCI Software's commitment to ensuring a secure and protected operational environment.	No Exceptions Noted
1.2.2	How Fire drill should be conducted annually.	Not Applicable	Not Applicable
1.2.3	Uninterruptible power supply (UPS) devices must be in place to secure critical IT equipment against power failures	During the audit of JASCI Software, it was observed that the company has established and maintained a comprehensive Physical Security Policy. This policy outlines the measures and controls in place to safeguard the organization's physical assets, infrastructure, and personnel, demonstrating JASCI Software's commitment to ensuring a secure and protected operational environment.	No Exceptions Noted
1.2.4	How many ISPs are in place to provide redundancy in case of link failure	During the audit of JASCI Software, it was observed that the company has maintained an up-to-date network diagram. This document provides a clear and detailed representation of the organization's network architecture, demonstrating JASCI Software's commitment to effective network management and security.	No Exceptions Noted
1.2.5	IS Backup policy defined in the information security policies	During the audit of JASCI Software, it was observed that the company has established and maintained a comprehensive Backup Policy, with documented approval in place. This reflects JASCI Software's commitment to ensuring data availability and resilience through structured and formally authorized backup management practices.	No Exceptions Noted
1.2.6	Is the local office backup performed within the local data center	During the audit of JASCI Software, it was observed that the company has established and maintained a comprehensive Backup Policy, with documented approval in place. This reflects JASCI Software's commitment to ensuring data availability and resilience through structured and formally authorized backup management practices.	No Exceptions Noted
1.2.7	Manual backup systems	During the audit of JASCI Software, it was observed that the company has established and maintained a comprehensive Backup Policy, with documented approval in place. This reflects JASCI Software's commitment to ensuring data availability and resilience through structured and formally authorized backup management practices.	No Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
A1.3	**The entity tests recovery plan procedures supporting system recovery to meet its objectives.**		
1.3.1	Are Disaster Recovery and Business Continuity plans and procedures documented for various disruption scenarios	During the audit of JASCI Software, it was observed that the company had maintained a well-defined Disaster Recovery Plan (DRP). This plan outlined the procedures to be followed in the event of disruptions, ensuring the continued operation of critical business functions.	No Exceptions Noted
1.3.2	Are business continuity plans, which include the restoration of backups, tested at least annually	During the audit of JASCI Software, it was observed that the company had maintained a well-defined Business Continuity Plan (BCP). This plan outlined the procedures to be followed in the event of disruptions, ensuring the continued operation of critical business functions.	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.**		
1.1.1	Has the entity established written policies related to retention periods, specifically the Procedure for Control of Documents and Records, for the confidential information it maintains? Additionally, does the entity securely destroy or delete all data as soon as it is no longer needed in accordance with these policies	During the audit of JASCI Software, it was observed that the company has established and maintained a Data Retention Policy, with documented approval in place. This demonstrates JASCI Software's commitment to effective data management and compliance with applicable regulatory and organizational requirements.	No Exceptions Noted
C1.2	**The entity disposes of confidential information to meet the entity's objectives related to confidentiality.**		
1.2.1	Do written policies related to retention periods, specifically outlined in the Procedure for Control of Documents and Records, exist within the entity for confidential information maintenance? Furthermore, does the entity ensure the secure destruction or deletion of all data as soon as it is no longer needed, in accordance with these policies	During the audit of JASCI Software, it was observed that the company has established and maintained a Data Disposal Policy, with documented approval in place. This highlights JASCI Software's commitment to secure and compliant data lifecycle management, ensuring proper and responsible disposal of data in alignment with regulatory and organizational requirements.	No Exceptions Noted

CRITERIA FOR PROCESSING INTEGRITY			
PI1.1	**The entity obtains or generates, uses, and communicates relevant, quality information regarding th e objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.**		
1.1.1	System Changes should be tested by appropriate individuals. Testing report should be documented and deviations from planned results must analyzed and remediated.	During the audit of JASCI Software, it was observed that the company has maintained an approved test plan, documented testing results, and records of changes. This demonstrates JASCI Software's commitment to structured testing processes, thorough documentation, and effective change management to ensure the reliability and quality of its systems and operations.	No Exceptions Noted
1.1.2	System alerts should be analyzed on a semi-annual basis to co-relate them. Further, the problem management process must invoked basis the result of investigation and correlation.	During the audit of JASCI Software, it was observed that the company provided comprehensive deployment evidence. This demonstrates JASCI Software's commitment to maintaining a well-documented and transparent deployment process, ensuring that all system changes and updates are effectively tracked and verified.	No Exceptions Noted
1.1.3	Monthly trend reports should be reviewed by the respective lead for unusual trends and problems must be created basis of the result of the review (if any)	During the audit of JASCI Software, it was observed that the company provided evidence of monthly trend email communications. This demonstrates JASCI Software's commitment to regular and transparent communication, ensuring that key trends and insights are effectively shared with relevant stakeholders.	No Exceptions Noted
1.1.4	Daily incremental backups should be performed using an automated system.	During the audit of JASCI Software, it was observed that the company has established and maintained a comprehensive Backup Policy, with documented approval in place. This reflects JASCI Software's commitment to ensuring data availability and resilience through structured and formally authorized backup management practices.	No Exceptions Noted
1.1.5	Processing capacity must be monitored on a monthly basis and forecasted to meet the business requirement.	During the audit of JASCI Software, it was observed that the company provided evidence of server monitoring. This demonstrates JASCI Software's commitment to proactively managing and monitoring server performance, ensuring the reliability and availability of its systems.	No Exceptions Noted

1.1.6	Logical access to stored data must be restricted only to the appropriate administrators.	During the audit of JASCI Software, it was observed that the company has maintained a comprehensive Access Control Policy. This policy outlines the measures and controls in place to manage and restrict access to sensitive information and systems, ensuring that only authorized personnel have access based on their roles and responsibilities.	No Exceptions Noted
PI1.2	**The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.**		
1.2.1	A mirror image of critical data files must be replicated periodically and stored on the second system for use in recovery and restoration in the event of system disruption or outage.	During the audit of JASCI Software, it was observed that the company has established and maintained a comprehensive Backup Policy, with documented approval in place. This reflects JASCI Software's commitment to ensuring data availability and resilience through structured and formally authorized backup management practices.	No Exceptions Noted
1.2.2	External access to an entity's environment by employees should be permitted only through an encrypted virtual private network (VPN) connection.	During the audit of JASCI Software, it was observed that the company has maintained a comprehensive Remote Access Policy. This policy defines the controls and guidelines for securely managing remote access to the organization's systems and data, ensuring that remote connections are conducted in a controlled and secure manner.	No Exceptions Noted
PI1.3	**The entity implements policies and procedures over system processing to result in products, service s, and reporting to meet the entity's objectives.**		
1.3.1	System Changes should be tested by appropriate individuals. Testing report should be documented and deviations from planned results should be analyzed and remediated.	During the audit of JASCI Software, it was observed that the company has maintained an approved test plan, documented testing results, and records of changes. This demonstrates JASCI Software's commitment to structured testing processes, thorough documentation, and effective change management to ensure the reliability and quality of its systems and operations.	No Exceptions Noted
1.3.2	System alerts should be analyzed on a semi-annual basis to co-relate them. Further, the problem management process should be invoked basis the result of investigation and correlation.	During the audit of JASCI Software, it was observed that the company provided evidence of infrastructure monitoring. This demonstrates JASCI Software's commitment to maintaining the health and performance of its infrastructure through continuous monitoring, ensuring the stability and reliability of its systems.	No Exceptions Noted

PI1.4	**The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.**		
1.4.1	Daily incremental backups should be performed using an automated system.	During the audit of JASCI Software, it was observed that the company has established and maintained a comprehensive Backup Policy, with documented approval in place. This reflects JASCI Software's commitment to ensuring data availability and resilience through structured and formally authorized backup management practices.	No Exceptions Noted
PI1.5	**The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.**		
1.5.1	Backups should be monitored for failure and the incident management process should be invoked whenever applicable to ensure timely resolution of issues and availability of the backup system.	During the audit of JASCI Software, it was observed that the company has established and maintained a comprehensive Backup Policy, with documented approval in place. This reflects JASCI Software's commitment to ensuring data availability and resilience through structured and formally authorized backup management practices.	No Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
ADDITIONAL CRITERIA FOR PRIVACY			
P1.0	**Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy**		
P1.1	**The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.**		
1.1.1	From the privacy perspective, the entity acts as the Processor or Sub-Processor of data shared by its clients. The entity does not collect, host, or store such data, the only access to it is remote.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
1.1.2	Outside the scope of Privacy, the entity processes data collected via its website as well as candidate and employee data. The entity communicates and provides notice of its privacy policy and practices to external data subjects via the website, and to internal data subjects via Confluence.	During the audit of JASCI Software, it was observed that the company has maintained a comprehensive Privacy Policy, which is publicly available on their company website. This demonstrates JASCI Software's commitment to transparency and compliance with privacy regulations, ensuring that stakeholders are informed about the company's data protection practices.	No Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
P2.0	**Privacy Criteria Related to Choose and Consent**		
P2.1	**The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.**		
2.1.1	The Entity website contains published privacy policies with information about choices available to data subjects.	During the audit of JASCI Software, it was observed that the company has maintained a comprehensive Privacy Policy, which is publicly available on their company website. This demonstrates JASCI Software's commitment to	No Exceptions Noted

		transparency and compliance with privacy regulations, ensuring that stakeholders are informed about the company's data protection practices.	
P3.0	**Privacy Criteria Related to Collection**		
P3.1	**Personal information is collected consistent with the entity's objectives related to privacy.**		
3.1.1	The entity does not define the scope of data its clients are providing. Entity's clients are companies sharing data subject to privacy laws applicable to them.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
P3.2	**For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.**		
Ref No	**Controls Implemented by Entity**	**Test Procedures**	**Test Results**
3.2.1	As a Processor or Sub-Processor, an entity does not collect any personal data. The entity processes data collected by the client, who is responsible for obtaining explicit consent or any form of consent, in line with applicable laws.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
P4.0	**Privacy Criteria Related to Use, Retention, and Disposal**		
P4.1	**The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.**		

4.1.1	Entity limits the processing of personal information to the minimum necessary to provide the service.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
P4.2	**The entity retains personal information consistent with the entity's objectives related to privacy.**		
4.2.1	Where legally required, the entity has documented policies for data retention to ensure that personal information is retained as per the data retention period and is protected from erasure or destruction during the period of retention.	During the audit of JASCI Software, it was observed that the company has established and maintained a Data Retention Policy, with documented approval in place. This demonstrates JASCI Software's commitment to effective data management and compliance with applicable regulatory and organizational requirements.	No Exceptions Noted
P4.3	**The entity securely disposes of personal information to meet the entity's objectives related to privacy.**		
4.3.1	As a processor, the entity does not process data subject requests for deletion. All requests are forwarded to the client for processing.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
4.3.2	The entity has documented policies for data retention to ensure that personal information is retained as per the data retention period and is protected from erasure or destruction during the period of retention.	During the audit of JASCI Software, it was observed that the company has established and maintained a Data Retention Policy, with documented approval in place. This demonstrates JASCI Software's commitment to effective data management and compliance with applicable regulatory and organizational requirements.	No Exceptions Noted
P5.0	**Privacy Criteria Related to Access**		
P5.1	**The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provide physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.**		
5.1.1	As a Processor, an entity does not process data subject requests - they have to be handled by the Controllers. Any requests received directly by the entity are forwarded to the clients for them to handle.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
P5.2	**The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and the reason for such denial to meet the entity's objectives related to privacy.**		
5.1.1	As a Processor, the entity does not process data subject requests for amendment to personal data - they have to be handled by the Controllers. Any requests received directly by the entity are forwarded to the clients for them to handle.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
P6.0	**Privacy Criteria Related to Disclosure and Notification**		

P6.1	The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
6.1.1	Entity communicates data protection and privacy policies to third parties to whom personal information is disclosed.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
6.1.2	An entity discloses personal information to third parties only when appropriate and for the purposes for which it was collected.	During the audit of JASCI Software, it was observed that the company has maintained a Data Sharing Agreement. This demonstrates JASCI Software's commitment to ensuring proper data handling and sharing practices, in compliance with applicable regulations and internal policies, to protect sensitive information when shared with third parties.	No Exceptions Noted
P6.2	**The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.**		
6.2.1	Entity creates and retains a record of authorized disclosures of personal information. A list of sub- processors is maintained.	During the audit of JASCI Software, it was observed that the company has maintained a Data Sharing Agreement. This demonstrates JASCI Software's commitment to ensuring proper data handling and sharing practices, in compliance with applicable regulations and internal policies, to protect sensitive information when shared with third parties.	No Exceptions Noted
P6.3	**The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.**		
6.3.1	Information security incidents are reported and logged as tickets. These incidents are classified by the type of incidents. Privacy incidents are also reported as part of this process.	Not Applicable	Not Applicable

Ref No	Controls Implemented by Entity	Test Procedures	Test Results

P6.4	**The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as- needed basis and takes corrective action, if necessary.**		
6.4.1	Entity obtains privacy commitments from vendors using Data Protection Agreement (DPA) with standard contract clauses. An entity discloses personal information only to appropriate third parties based on the purpose of the information.	During the audit of JASCI Software, it was observed that the company has maintained both a Data Sharing Agreement and a Data Protection Agreement. This demonstrates JASCI Software's commitment to safeguarding sensitive information through clearly defined terms for data sharing and protection, ensuring compliance with relevant data privacy regulations and best practices.	No Exceptions Noted
P6.5	**The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy.**		
6.5.1	Entity obtains commitments from vendors and other third parties for the management of information security incidents, including unauthorized disclosure of personal information.	During the audit of JASCI Software, it was observed that the company has maintained both a Data Sharing Agreement and a Data Protection Agreement. This demonstrates JASCI Software's commitment to safeguarding sensitive information through clearly defined terms for data sharing and protection, ensuring compliance with relevant data privacy regulations and best practices.	No Exceptions Noted

Ref No	Controls Implemented by Entity	Test Procedures	Test Results
P6.6	**The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.**		
6.6.1	Breach notification procedures are documented and reviewed on a periodic basis.	During the audit of JASCI Software, it was observed that the company has maintained a comprehensive Incident Response Plan. This plan outlines the procedures and protocols for effectively addressing and managing security incidents, demonstrating JASCI Software's commitment to minimizing the impact of incidents and ensuring a timely and coordinated response.	No Exceptions Noted
6.6.2	The entity takes remedial action in response to breaches and incidents when it involves personal information.	During the audit of JASCI Software, it was observed that the company has maintained a comprehensive Incident Response Plan. This plan outlines the procedures and protocols for effectively addressing and managing security incidents, demonstrating JASCI Software's commitment to minimizing the impact of incidents and ensuring a timely and coordinated response.	No Exceptions Noted
P6.7	**The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subject's request, to meet the entity's objectives related to privacy.**		
6.7.1	As a Processor, the entity does not process data subject requests - they have to be handled by the Controllers. Any requests received directly by the entity are forwarded to the clients for them to handle.	During the audit of JASCI Software, it was observed that the company has maintained both a Data Sharing Agreement and a Data Protection Agreement. This demonstrates JASCI Software's commitment to safeguarding sensitive information through clearly defined terms for data sharing and protection, ensuring compliance with relevant data privacy regulations and best practices.	No Exceptions Noted
P7.0	**Privacy Criteria Related to Quality**		

P7.1	**The entity collects and maintains accurate, up-to- date, complete, and relevant personal information to meet the entity's objectives related to privacy.**		
7.1.1	As a Processor, the entity does not host nor store any client data - any access to client data is remote. The entity does not carry out procedures to maintain it accurate and up to date, it is the client's responsibility.	During the audit of JASCI Software, it was observed that the company provided a Statement of Work (SOW), a Support Services document, and evidence of a Master Subscription Agreement (MSA). This demonstrates JASCI Software's commitment to formalizing its service agreements and ensuring clear, structured terms for the delivery of services and support to clients.	No Exceptions Noted
P 8.0	**Privacy Criteria Related to Monitoring and Enforcement**		
P 8.1	**The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.**		
	Privacy data incidents are reported to management as and when they occur.	During the audit of JASCI Software, it was observed that the company has maintained a comprehensive Privacy Policy. This policy reflects JASCI Software's commitment to protecting personal data and ensuring compliance with privacy regulations, outlining how personal information is collected, used, and safeguarded.	No Exceptions Noted

----------End of the Report----------