CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Introduction

Consensus Assessments Initiative Questionnaire (CAIQ):

This tab includes the questionnaire associated with the Cloud Control Matrix (CCM) controls, commonly known as the CAIQ.

The Consensus Assessments Initiative Questionnaire version 4 (or CAIQv4.0.2) aligns with the CCMv4.0.2 control specifications. The CAIQv4.0.2's purpose is to help organizations conduct self-assessments to test their compliance against the CCM V4. It is developed under CSA's STAR-Level 1 program umbrella, allowing organizations to complete and submit self-assessments to CSA's STAR Registry.

The CAIQv4.0.2 features 261 questions structured and formulated based on the 17 domains and underlying control specifications of the CCM.

Each question is described using the following attributes:

Question ID

The question identifiers.

Assessment Question

The description of the question.

In addition, this tab includes the following sections (groups of columns).

CSP CAIQ Answer

The Cloud Service Provider (CSP) must respond with "Yes"/ "No"/ "NA" next to the corresponding assessment question, and for the portion(s) of the CCM control specification they are responsible and accountable for implementing.

Meaning of possible replies:

• "Yes": The portion(s) of the CCM control requirement corresponding to the assessment question is met.

• "No": The portion(s) of the CCM control requirement corresponding to the assessment question is not met.

• "N/A": The question is not in scope and does not apply to the cloud service under assessment.

NOTES:
A "Yes" answer indicates that the portion of the control in question is implemented. The CSP indicates the responsible and accountable parties (SSRM control ownership), and optionally elaborates on the implementation "how-to" per relevant party CSP and/or CSC.

A "No" answer indicates that the portion of the control in question is not implemented, while in scope of the assessment. The CSP has to assign the implementation responsibility of the control to the relevant party under column "SSRM control ownership", and optionally elaborate on the "why" (has not been implemented), and "what" has to be done for its implementation by that party.

A "N/A" answer indicates that the portion of the control in question is out of scope of the assessment. The "SSRM control ownership" column is to be left blank (e.g., greyed out), and optionally the CSP may explain why it is the case ("CSP Implementation Description").

Shared Security Responsibility Model (SSRM) control ownership

The CSP control responses shall identify control applicability and ownership for their specific service.

• CSP-owned: The CSP is entirely responsible and accountable for the CCM control implementation.

• CSC-owned: The Cloud Service Customer (CSC) is entirely responsible and accountable for the CCM control implementation.

• Third-party outsourced: The third-party CSP in the supply chain (e.g., an IaaS provider) is responsible for CCM control implementation, while the CSP is fully accountable.

• Shared CSP and CSC: Both the CSP and CSC share CCM control implementation responsibility and accountability.

• Shared CSP and third party: Any CCM control implementation responsibility is shared between CSP and the third party, but the CSP remains fully accountable.

Note: The CAIQv4 SSRM schema is tailored to CCMv4's Supply Chain Management, Transparency, and Accountability (STA) domain, controls 1-6, and their corresponding implementation guidelines.

CSP implementation description (optional/recommended)

A description (with references) of how the cloud service provider meets (or does not meet) the portion(s) of the SSRM control they are responsible for. If "NA," explain why.

CSC responsibilities (optional/recommended)

A summary description of the cloud service customer security responsibilities for the portion(s) of the SSRM control that is responsible for, with corresponding guidance and references.

End of Introduction

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Chargebee has a well-defined set of Information Security Policies and supporting procedures & guidelines aligned to ISO 27001:2013 standard. All policies and procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement. Policies are published internally in Chargebee's intranet portal and are made accessible to all the employees.	Not Applicable as the control is owned by CSP (Chargebee)	A&A-01	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually.	Audit and Assurance Policy and Procedures	Audit & Assurance
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?	Yes	CSP-owned	Chargebee undergoes an external audit as part of its ISO 27001:2013 certification and a SOC 2 Type II attestation covering Security as on of the Trust Service Criteria. These audits / certifications are performed by	Not Applicable as the control is owned by CSP (Chargebee)	A&A-02	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independent Assessments	
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies?	Yes	CSP-owned	Chargebee performs annual risk assessment and results from risk assessment activities are reviewed to prioritize mitigation of identified risks. This also covered as part of ISO 27001 audit.	Not Applicable as the control is owned by CSP (Chargebee)	A&A-03	Perform independent audit and assurance assessments according to risk-based plans and policies.	Risk Based Planning Assessment	
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?	Yes	Shared CSP and CSC	Chargebee has Risk and Compliance team which verifies and aligns policies and process with all relevant standards, regulations , legalcontractual and statutory requirements.	Merchants are advised to verify their due-diligence as per the regulations applicable to their region/business. Merchants can review the compliance certificates/reports from the security page here.	A&A-04	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requirements Compliance	
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence?	Yes	CSP-owned	Chargebee has a dedicated Risk and Compliance team who is responsible for conducting the internal audit on a periodic based on the framework. Management review meetings are conducted on a periodic basis to discuss the findings and way forward. The team has a documented process to track and reports the remediation of	Not Applicable as the control is owned by CSP (Chargebee)	A&A-05	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Audit Management Process	
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Chargebee has developed a Risk Management Framework as part of the Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2013 standard.	Not Applicable as the control is owned by CSP (Chargebee)	A&A-06	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	Remediation	
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?	Yes	CSP-owned	Risks identified during the risk assessment are recorded within the Risk Assessment register and Risk Management Dashboard. All the identified risks are mapped to a risk owner, and risk treatment plans are	Not Applicable as the control is owned by CSP (Chargebee)				
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?	Yes	CSP-owned	Application Security Policies are established and are part of Chargebee's Information Security Policies and supporting procedures & guidelines which is aligned to ISO 27001:2013 standard. All policies and procedures are reviewed at least annually or when there is a significant change in the business, technology,	Not Applicable as the control is owned by CSP (Chargebee)	AIS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	Application and Interface Security Policy and Procedures	Application & Interface Security
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?	Yes	CSP-owned	Chargebee employs secure coding techniques and best practices recommended in OWASP and SANS methodologies in defining the baseline requirements to secure all its applications.All our standards and	Not Applicable as the control is owned by CSP (Chargebee)	AIS-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?	Yes	CSP-owned	Technical and operational metrics are defined and implemented.	Not Applicable as the control is owned by CSP (Chargebee)	AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?	Yes	CSP-owned	Chargebee follows a clearly defined change management cycle for deploying code changes to the Chargebee's application. Our development team employs secure coding techniques and best practices	Not Applicable as the control is owned by CSP (Chargebee)	AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?	Yes	CSP-owned	Please refer to CSP Implementation Description in AIS-04.1	Not Applicable as the control is owned by CSP (Chargebee)	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application Security Testing	
AIS-05.2	Is testing automated when applicable and possible?	Yes	CSP-owned	Please refer to CSP Implementation Description in AIS-04.1	Not Applicable as the control is owned by CSP (Chargebee)				
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?	Yes	CSP-owned	Chargebee change control processes ensure that only approved changes are deployed to production. This includes verifying functional and security testing results before deployment. Chargebee follows a clearly defined change	Not Applicable as the control is owned by CSP (Chargebee)	AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	
AIS-06.2	Is the deployment and integration of application code automated where possible?	Yes	CSP-owned	Chargebee uses Terraform for resource deployment, CI/CD and internal deployment tools for application code.	Not Applicable as the control is owned by CSP (Chargebee)				
AIS-07.1	Are application security vulnerabilities remediated following defined processes?	Yes	CSP-owned	Chargebee has defined and documented a formal Vulnerability Management Policy and Procedure to provide a common set of methodologies and requirements to	Not Applicable as the control is owned by CSP (Chargebee)	AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?	Yes	CSP-owned	Please refer to CSP Implementation Description in AIS-07.1	Not Applicable as the control is owned by CSP (Chargebee)				
BCR-01.1	Are business continuity management and operational resilience policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Chargebee has developed a formal Business Continuity Plan (BCP) to minimise disruption to critical services in times of crisis and to maintain a higher degree of resilience. Crisis roles and responsibilities are defined as part of the BCP plan. The BCP and DR plan of Chargebee are reviewed and	Not Applicable as the control is owned by CSP (Chargebee)	BCR-01	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	Business Continuity Management Policy and Procedures	
BCR-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
BCR-02.1	Are criteria for developing business continuity and operational resiliency strategies and capabilities established based on business disruption and risk impacts?	Yes	CSP-owned	Business Impact analysis is performed to identify critical operations, processes and facilities and forms part of the BCP planning.	Not Applicable as the control is owned by CSP (Chargebee)	BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	Risk Assessment and Impact Analysis	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
BCR-03.1	Are strategies developed to reduce the impact of, withstand, and recover from business disruptions in accordance with risk appetite?	Yes	CSP-owned	Please refer to CSP Implementation Description in BCR-02.1	Not Applicable as the control is owned by CSP (Chargebee)	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	Business Continuity Strategy	Business Continuity Management and Operational Resilience
BCR-04.1	Are operational resilience strategies and capability results incorporated to establish, document, approve, communicate, apply, evaluate, and maintain a business continuity plan?	Yes	CSP-owned	Please refer to CSP Implementation Description in BCR-01.1	Not Applicable as the control is owned by CSP (Chargebee)	BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	Business Continuity Planning	
BCR-05.1	Is relevant documentation developed, identified, and acquired to support business continuity and operational resilience plans?	Yes	CSP-owned	Chargebee has developed a formal Business Continuity Plan (BCP) and Disaster Recovery (DR) plan to minimize disruption to critical services in times of crisis and to maintain a higher degree of resilience. Crisis roles	Not Applicable as the control is owned by CSP (Chargebee)	BCR-05	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically.	Documentation	
BCR-05.2	Is business continuity and operational resilience documentation available to authorized stakeholders?	Yes	CSP-owned	Yes, the executive summary of BCP and DR plan in made available to authorized stakeholders upon request.	Not Applicable as the control is owned by CSP (Chargebee)				
BCR-05.3	Is business continuity and operational resilience documentation reviewed periodically?	Yes	CSP-owned	BCP plan is documented and reviewed at least annually or whenever there is a major change in the process or control.	Not Applicable as the control is owned by CSP (Chargebee)				
BCR-06.1	Are the business continuity and operational resilience plans exercised and tested at least annually and when significant changes occur?	Yes	CSP-owned	DR plan is tested on an annual basis or whenever a significant change occurs.	Not Applicable as the control is owned by CSP (Chargebee)	BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	Business Continuity Exercises	
BCR-07.1	Do business continuity and resilience procedures establish communication with stakeholders and participants?	Yes	CSP-owned	BCP Plan/DR plan includes procedures for communication with stakeholders and participants.	Not Applicable as the control is owned by CSP (Chargebee)	BCR-07	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures.	Communication	
BCR-08.1	Is cloud data periodically backed up?	Yes	Shared CSP and 3rd-party	Chargebee has a Backup policy in place to ensure that backup copies of essential business information, data, and support information are taken regularly in a manner such that it is available for restoration of business operations whenever required within the stipulated time	Not Applicable as the control is owned by CSP (Chargebee)	BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	Backup	
BCR-08.2	Is the confidentiality, integrity, and availability of backup data ensured?	Yes	Shared CSP and 3rd-party	All backups are stored in an encrypted manner and are tested regularly to ensure the integrity of the back-up data.	Not Applicable as the control is owned by CSP (Chargebee)				
BCR-08.3	Can backups be restored appropriately for resiliency?	Yes	Shared CSP and 3rd-party	Chargebee has a defined process in place to restore backups for resiliency.	Not Applicable as the control is owned by CSP (Chargebee)				
BCR-09.1	Is a disaster response plan established, documented, approved, applied, evaluated, and maintained to ensure recovery from natural and man-made disasters?	Yes	CSP-owned	Chargebee has developed a formal Business Continuity Plan (BCP) and Disaster Recovery (DR) plan to minimize disruption to critical services in times of crisis and to maintain a higher degree of resilience. Crisis roles	Not Applicable as the control is owned by CSP (Chargebee)	BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	Disaster Response Plan	
BCR-09.2	Is the disaster response plan updated at least annually, and when significant changes occur?	Yes	CSP-owned	Yes, the Disaster Recovery (DR) plan is reviewed and updated at least annually, and/or when a significant change occur.	Not Applicable as the control is owned by CSP (Chargebee)				
BCR-10.1	Is the disaster response plan exercised annually or when significant changes occur?	Yes	CSP-owned	Please refer to CSP Implementation Description in BCR-09.2	Not Applicable as the control is owned by CSP (Chargebee)	BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	Response Plan Exercise	
BCR-10.2	Are local emergency authorities included, if possible, in the exercise?	Yes	CSP-owned	Yes, all the required stakeholders are included in the exercise.	Not Applicable as the control is owned by CSP (Chargebee)				
BCR-11.1	Is business-critical equipment supplemented with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards?	Yes	CSP-owned	Chargebee uses Amazon's AWS platform and infrastructure which operates on highly-available and fault tolerant data centres. Amazon RDS has been configured in Multi-AZ located regions. Each AZ runs on its own physically distinct, independent infrastructure and enhanced availability and durability at Web, Application and	Not Applicable as the control is owned by CSP (Chargebee)	BCR-11	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards.	Equipment Redundancy	
CCC-01.1	Are risk management policies and procedures associated with changing organizational assets including applications, systems, infrastructure, configuration, etc., established, documented, approved, communicated, applied, evaluated and maintained (regardless of whether asset management is internal or external)?	Yes	CSP-owned	Chargebee has established a formal change management program to ensure formal process is followed for making any changes to systems/ applications. This includes a defined Change Approval Matrix for handling / managing any exception to the process. All policies and procedures are reviewed at least annually or when there is a significant change in the	Not Applicable as the control is owned by CSP (Chargebee)	CCC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually.	Change Management Policy and Procedures	Change Control and Configuration Management
CCC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
CCC-02.1	Is a defined quality change control, approval and testing process (with established baselines, testing, and release standards) followed?	Yes	CSP-owned	Chargebee has established a formal change management program to ensure formal process is followed for making any changes to systems/ applications. Development, staging and production environments are	Not Applicable as the control is owned by CSP (Chargebee)	CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	Quality Testing	
CCC-03.1	Are risks associated with changing organizational assets (including applications, systems, infrastructure, configuration, etc.) managed, regardless of whether asset management occurs internally or externally (i.e., outsourced)?	Yes	CSP-owned	Please refer to CSP Implementation Description in CCC-01.1	Not Applicable as the control is owned by CSP (Chargebee)	CCC-03	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced).	Change Management Technology	
CCC-04.1	Is the unauthorized addition, removal, update, and management of organization assets restricted?	Yes	CSP-owned	Yes, Administrative access with the privilege to perform changes (addition, removal, update and management of organization assets) are assigned to select members based on roles and	Not Applicable as the control is owned by CSP (Chargebee)	CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	Unauthorized Change Protection	
CCC-05.1	Are provisions to limit changes that directly impact CSC-owned environments and require tenants to authorize requests explicitly included within the service level agreements (SLAs) between CSPs and CSCs?	NA	CSP-owned	Changes applied to the cloud environment is mandatory for all customers. Hence, the customer cannot refuse the changes carried out by Chargebee.	Not Applicable as the control is owned by CSP (Chargebee)	CCC-05	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs.	Change Agreements	
CCC-06.1	Are change management baselines established for all relevant authorized changes on organizational assets?	Yes	CSP-owned	Please refer to CSP Implementation Description in CCC-01.1	Not Applicable as the control is owned by CSP (Chargebee)	CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	Change Management Baseline	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CCC-07.1	Are detection measures implemented with proactive notification if changes deviate from established baselines?	Yes	CSP-owned	Please refer to CSP Implementation Description in CCC-01.1	Not Applicable as the control is owned by CSP (Chargebee)	CCC-07	Implement detection measures with proactive notification in case of changes deviating from the established baseline.	Detection of Baseline Deviation	
CCC-08.1	Is a procedure implemented to manage exceptions, including emergencies, in the change and configuration process?	Yes	CSP-owned	Our Change management procedures includes various aspects including managing exceptions, emergency changes, backout plans, impact analysis etc. This also includes a defined Change Approval Matrix for [illegible]	Not Applicable as the control is owned by CSP (Chargebee)	CCC-08	'Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process.'	Exception Management	
CCC-08.2	'Is the procedure aligned with the requirements of the GRC-04: Policy Exception Process?'	Yes	CSP-owned	For any exceptions or deviations to the organization's information security policy, the additional risk introduced from the deviation would be analysed and treated by implementing appropriate additional / compensating controls. This [illegible]	Not Applicable as the control is owned by CSP (Chargebee)				
CCC-09.1	Is a process to proactively roll back changes to a previously known "good state" defined and implemented in case of errors or security concerns?	Yes	CSP-owned	Please refer to CSP Implementation Description in CCC-08.1	Not Applicable as the control is owned by CSP (Chargebee)	CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	Change Restoration	
CEK-01.1	Are cryptography, encryption, and key management policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	Chargebee has a defined Cryptography & Key Management Policy & Procedure aligned to ISO 27001:2013 standard. All policies and procedures are reviewed at least annually or when there is a significant [illegible]	Not Applicable as the control is owned by CSP (Chargebee)	CEK-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually.	Encryption and Key Management Policy and Procedures	
CEK-01.2	Are cryptography, encryption, and key management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
CEK-02.1	Are cryptography, encryption, and key management roles and responsibilities defined and implemented?	Yes	Shared CSP and 3rd-party	Chargebee leverages on AWS KMS for managing lifecycle of encryption keys. AWS establishes and manages cryptographic keys for required cryptography employed within the	Not Applicable as the control is owned by CSP (Chargebee)	CEK-02	Define and implement cryptographic, encryption and key management roles and responsibilities.	CEK Roles and Responsibilities	
CEK-03.1	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	CSP-owned	Data is encrypted at rest. The keys for various third party services (like payment gateway) are stored in our database in encrypted form. We use the AWS Managed Keys - KMS for RDS Encryption and they are AES 256 [illegible]	Not Applicable as the control is owned by CSP (Chargebee)	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.	Data Encryption	
CEK-04.1	Are appropriate data protection encryption algorithms used that consider data classification, associated risks, and encryption technology usability?	Yes	CSP-owned	Please refer to CSP Implementation Description in CEK-03.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-04	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology.	Encryption Algorithm	
CEK-05.1	Are standard change management procedures established to review, approve, implement and communicate cryptography, encryption, and key management technology changes that accommodate internal and external sources?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-05	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes.	Encryption Change Management	
CEK-06.1	Are changes to cryptography-, encryption- and key management-related systems, policies, and procedures, managed and adopted in a manner that fully accounts for downstream effects of proposed changes, including residual risk, cost, and benefits analysis?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-06	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis.	Encryption Change Cost Benefit Analysis	
CEK-07.1	Is a cryptography, encryption, and key management risk program established and maintained that includes risk assessment, risk treatment, risk context, monitoring, and feedback provisions?	Yes	CSP-owned	Chargebee's Risk management program covers these aspects.	Not Applicable as the control is owned by CSP (Chargebee)	CEK-07	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback.	Encryption Risk Management	
CEK-08.1	Are CSPs providing CSCs with the capacity to manage their own data encryption keys?	No	Shared CSP and 3rd-party	Encryption keys are managed by Chargebee using AWS Key management service. Currently, we do not support customer owned/managed keys.	Not Applicable as the control is owned by CSP (Chargebee)	CEK-08	CSPs must provide the capability for CSCs to manage their own data encryption keys.	CSC Key Management Capability	
CEK-09.1	Are encryption and key management systems, policies, and processes audited with a frequency proportional to the system's risk exposure, and after any security event?	Yes	CSP-owned	This is audited as part of SOC 2 Type 2 assessment, ISO 27001 and/or as needed after any security event/incident.	Not Applicable as the control is owned by CSP (Chargebee)	CEK-09	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s).	Encryption and Key Management Audit	
CEK-09.2	Are encryption and key management systems, policies, and processes audited (preferably continuously but at least annually)?	Yes	CSP-owned	Please refer to CSP Implementation Description in CEK-09.1	Not Applicable as the control is owned by CSP (Chargebee)				
CEK-10.1	Are cryptographic keys generated using industry-accepted and approved cryptographic libraries that specify algorithm strength and random number generator specifications?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-10	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used.	Key Generation	
CEK-11.1	Are private keys provisioned for a unique purpose managed, and is cryptography secret?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-11	Manage cryptographic secret and private keys that are provisioned for a unique purpose.	Key Purpose	
CEK-12.1	Are cryptographic keys rotated based on a cryptoperiod calculated while considering information disclosure risks and legal and regulatory requirements?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-12	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements.	Key Rotation	Cryptography, Encryption & Key Management
CEK-13.1	Are cryptographic keys revoked and removed before the end of the established cryptoperiod (when a key is compromised, or an entity is no longer part of the organization) per defined, implemented, and evaluated processes, procedures, and technical measures to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-13	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements.	Key Revocation	
CEK-14.1	Are processes, procedures and technical measures to destroy unneeded keys defined, implemented and evaluated to address key destruction outside secure environments, revocation of keys stored in hardware security modules (HSMs), and include applicable legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-14	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements.	Key Destruction	
CEK-15.1	Are processes, procedures, and technical measures to create keys in a pre-activated state (i.e., when they have been generated but not authorized for use) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-15	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements.	Key Activation	
CEK-16.1	Are processes, procedures, and technical measures to monitor, review and approve key transitions (e.g., from any state to/from suspension) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-16	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements.	Key Suspension	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
CEK-17.1	Are processes, procedures, and technical measures to deactivate keys (at the time of their expiration date) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-17	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements.	Key Deactivation	
CEK-18.1	Are processes, procedures, and technical measures to manage archived keys in a secure repository (requiring least privilege access) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-18	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements.	Key Archival	
CEK-19.1	Are processes, procedures, and technical measures to encrypt information in specific scenarios (e.g., only in controlled circumstances and thereafter only for data decryption and never for encryption) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Data is encrypted at rest. We do not store sensitive card details on any Chargebee network. The keys for various third party services (like payment gateway) are stored in our database in encrypted form. All the data in our database is encrypted at rest. We use the AWS Managed Keys -	Not Applicable as the control is owned by CSP (Chargebee)	CEK-19	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements.	Key Compromise	
CEK-20.1	Are processes, procedures, and technical measures to assess operational continuity risks (versus the risk of losing control of keying material and exposing protected data) being defined, implemented, and evaluated to include legal and regulatory requirement provisions?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-20	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements.	Key Recovery	
CEK-21.1	Are key management system processes, procedures, and technical measures being defined, implemented, and evaluated to track and report all cryptographic materials and status changes that include legal and regulatory requirements provisions?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in CEK-02.1	Not Applicable as the control is owned by CSP (Chargebee)	CEK-21	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements.	Key Inventory Management	
DCS-01.1	Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?	Yes	3rd-party outsourced	Chargebee uses Amazon's AWS platform and infrastructure and hence this control is managed by AWS. Chargebee employees do not have any physical access to our production environment. Here are more details about the security setup of AWS. Cloud security is the highest priority at	Not Applicable as the control is owned by CSP (Chargebee)	DCS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually.	Off-Site Equipment Disposal Policy and Procedures	
DCS-01.2	Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)				
DCS-01.3	Are policies and procedures for the secure disposal of equipment used outside the organization's premises reviewed and updated at least annually?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)				
DCS-02.1	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location established, documented, approved, communicated, implemented, enforced, maintained?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location.The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually.	Off-Site Transfer Authorization Policy and Procedures	
DCS-02.2	Does a relocation or transfer request require written or cryptographically verifiable authorization?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)				
DCS-02.3	Are policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location reviewed and updated at least annually?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)				
DCS-03.1	Are policies and procedures for maintaining a safe and secure working environment (in offices, rooms, and facilities) established, documented, approved, communicated, enforced, and maintained?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually.	Secure Area Policy and Procedures	Datacenter Security
DCS-03.2	Are policies and procedures for maintaining safe, secure working environments (e.g., offices, rooms) reviewed and updated at least annually?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)				
DCS-04.1	Are policies and procedures for the secure transportation of physical media established, documented, approved, communicated, enforced, evaluated, and maintained?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually.	Secure Media Transportation Policy and Procedures	
DCS-04.2	Are policies and procedures for the secure transportation of physical media reviewed and updated at least annually?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)				
DCS-05.1	Is the classification and documentation of physical and logical assets based on the organizational business risk?	Yes	3rd-party outsourced	All customer data is stored and processed in AWS data centers. AWS classifies all storage media as 'confidential' and have implemented appropriate security measures to	Not Applicable as the control is owned by CSP (Chargebee)	DCS-05	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk.	Assets Classification	
DCS-06.1	Are all relevant physical and logical assets at all CSP sites cataloged and tracked within a secured system?	Yes	3rd-party outsourced	All customer data is stored and processed in AWS data centers. AWS is responsible for cataloging, labelling and tracking any physical and logical assets at the datacenter.	Not Applicable as the control is owned by CSP (Chargebee)	DCS-06	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system.	Assets Cataloguing and Tracking	
DCS-07.1	Are physical security perimeters implemented to safeguard personnel, data, and information systems?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-07	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas.	Controlled Access Points	

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DCS-07.2	Are physical security perimeters established between administrative and business areas, data storage, and processing facilities?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-07		Controlled Access Points	
DCS-08.1	Is equipment identification used as a method for connection authentication?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1 and DCS-06.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-08	Use equipment identification as a method for connection authentication.	Equipment Identification	
DCS-09.1	Are solely authorized personnel able to access secure areas, with all ingress and egress areas restricted, documented, and monitored by physical access control mechanisms?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-09	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization.	Secure Area Authorization	
DCS-09.2	Are access control records retained periodically, as deemed appropriate by the organization?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)				
DCS-10.1	Are external perimeter datacenter surveillance systems and surveillance systems at all ingress and egress points implemented, maintained, and operated?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-10	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts.	Surveillance System	
DCS-11.1	Are datacenter personnel trained to respond to unauthorized access or egress attempts?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-11	Train datacenter personnel to respond to unauthorized ingress or egress attempts.	Unauthorized Access Response Training	
DCS-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure risk-based protection of power and telecommunication cables from interception, interference, or damage threats at all facilities, offices, and rooms?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-12	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms.	Cabling Security	
DCS-13.1	Are data center environmental control systems designed to monitor, maintain, and test that on-site temperature and humidity conditions fall within accepted industry standards effectively implemented and maintained?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-13	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards.	Environmental Systems	
DCS-14.1	Are utility services secured, monitored, maintained, and tested at planned intervals for continual effectiveness?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-14	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals.	Secure Utilities	
DCS-15.1	Is business-critical equipment segregated from locations subject to a high probability of environmental risk events?	Yes	3rd-party outsourced	Please refer to CSP Implementation Description in DCS-01.1	Not Applicable as the control is owned by CSP (Chargebee)	DCS-15	Keep business-critical equipment away from locations subject to high probability for environmental risk events.	Equipment Location	
DSP-01.1	Are policies and procedures established, documented, approved, communicated, enforced, evaluated, and maintained for the classification, protection, and handling of data throughout its lifecycle according to all applicable laws and regulations, standards, and risk level?	Yes	CSP-owned	Chargebee has a defined Privacy policy that aligns with all applicable laws and regulations, standards, and risk level.	Not Applicable as the control is owned by CSP (Chargebee)	DSP-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	Security and Privacy Policy and Procedures	
DSP-01.2	Are data security and privacy policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
DSP-02.1	Are industry-accepted methods applied for secure data disposal from storage media so information is not recoverable by any forensic means?	Yes	Shared CSP and 3rd-party	For secure data disposal, any information contained inside CB devices are formatted before disposal. We degauss failed hard drives and then physically destroy them as per the	Not Applicable as the control is owned by CSP (Chargebee)	DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means.	Secure Disposal	
DSP-03.1	Is a data inventory created and maintained for sensitive and personal information (at a minimum)?	Yes	Shared CSP and CSC	We have separate data classification for PII / PCI information in our database. The customer's can manage these data based on their use cases using the CB product features/offerings.	The customer who is the data controller will decide what data to be processed. Chargebee acts be a data processor and will process the data based on customer's instructions.	DSP-03	Create and maintain a data inventory, at least for any sensitive data and personal data.	Data Inventory	
DSP-04.1	Is data classified according to type and sensitivity levels?	Yes	CSP-owned	Chargebee has determined the following four security classes for information classification based on the sensitivity level of the information	Not Applicable as the control is owned by CSP (Chargebee)	DSP-04	Classify data according to its type and sensitivity level.	Data Classification	
DSP-05.1	Is data flow documentation created to identify what data is processed and where it is stored and transmitted?	Yes	CSP-owned	Chargebee maintains a high level data flow documentation for our critical operations.	Not Applicable as the control is owned by CSP (Chargebee)	DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	Data Flow Documentation	
DSP-05.2	Is data flow documentation reviewed at defined intervals, at least annually, and after any change?	Yes	CSP-owned	Such data flows are reviewed as required or whenever there is a major change.	Not Applicable as the control is owned by CSP (Chargebee)				
DSP-06.1	Is the ownership and stewardship of all relevant personal and sensitive data documented?	Yes	Shared CSP and CSC	All personal and/or sensitive data are processed as per identified lawful basis. There is clear ownership and stewardship defined across organisation while processing personal	Customer is the owner of the data processed. Chargebee will be a data processor and will process the data as per the instructions of the data controller.	DSP-06	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually.	Data Ownership and Stewardship	
DSP-06.2	Is data ownership and stewardship documentation reviewed at least annually?	Yes	CSP-owned	Data ownership and stewardship are reviewed annually and if there is any major change/trigger in the PI processing.					
DSP-07.1	Are systems, products, and business practices based on security principles by design and per industry best practices?	Yes	CSP-owned	Chargebee follows "Security by design" approach in the planning and analysis phase of SDLC by way of incorporating security risk assessments and Threat modelling.	Not Applicable as the control is owned by CSP (Chargebee)	DSP-07	Develop systems, products, and business practices based upon a principle of security by design and industry best practices.	Data Protection by Design and Default	
DSP-08.1	Are systems, products, and business practices based on privacy principles by design and according to industry best practices?	Yes	CSP-owned	Chargebee applies privacy by design and default principles and our application is built in such a way to exercise data privacy rights (Eg: Right to access, right to rectification & erasure and right to data portability).	Not Applicable as the control is owned by CSP (Chargebee)	DSP-08	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	Data Privacy by Design and Default	
DSP-08.2	Are systems' privacy settings configured by default and according to all applicable laws and regulations?	Yes	Shared CSP and CSC	Chargebee applies privacy by design and default principles and our application is built in such a way to exercise data privacy rights. Our products adhere to GDPR and applicable privacy regulatory requirements and privacy settings / features are made available to our	Customers are responsible for configuring appropriate features in accordance with their applicable laws, regulations and privacy requirements.				
DSP-09.1	Is a data protection impact assessment (DPIA) conducted when processing personal data and evaluating the origin, nature, particularity, and severity of risks according to any applicable laws, regulations and industry best practices?	Yes	Shared CSP and CSC	As we are a data processor, we provide necessary and required assistance to our Merchants (controller) for conducting DPIA, as needed. As a SaaS product, we have required privacy features and TOMs deployed in the product which ensure data protection at our end, as well as enable merchants to use privacy	Data Protection Impact Assessment is the obligation of the Data Controller (i. e. merchant/customer) and Chargebee as a data processor, will provide necessary and required assistance to our Merchants (controller) for conducting DPIA.	DSP-09	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices.	Data Protection Impact Assessment	Data Security and Privacy

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
DSP-10.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope (as permitted by respective laws and regulations)?	Yes	CSP-owned	Chargebee has implemented and shall maintain appropriate Technical and Organisational Measures (TOMS).	Not Applicable as the control is owned by CSP (Chargebee)	DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	Sensitive Data Transfer	Lifecycle Management
DSP-11.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable data subjects to request access to, modify, or delete personal data (per applicable laws and regulations)?	Yes	Shared CSP and CSC	Chargebee has defined multiple channels to receive, and a single channel to address data subject requests. There are defined processes, systems, timelines, ownerships and responsibilities for addressing Data Subject Requests timely and satisfactorily, subject to the applicable	Chargebee has a defined process to follow in both cases - (i) Data subject request received directly from data subject and (ii) data subject request received by customer. In both cases, Chargebee will assist	DSP-11	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations.	Personal Data Access, Reversal, Rectification and Deletion	
DSP-12.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure personal data is processed (per applicable laws and regulations and for the purposes declared to the data subject)?	Yes	Shared CSP and CSC	Chargebee applies privacy by design and default principles and our application is built in such a way to exercise data privacy rights. Our products adhere to GDPR requirements and privacy settings / features are made available to our customers which can be enabled by	Customers are responsible for configuring appropriate features in accordance with their applicable laws, regulations and privacy requirements.	DSP-12	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject.	Limitation of Purpose in Personal Data Processing	
DSP-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for the transfer and sub-processing of personal data within the service supply chain (according to any applicable laws and regulations)?	Yes	Shared CSP and 3rd-party	Chargebee involves sub-processors as part of the services provided to our customers. We review the technical measures implemented by all our sub-processors in accordance with GDPR, and a mutually agreed Data Processing Addendum is also executed with all the sub-processors. A	Not Applicable as the control is owned by CSP (Chargebee)	DSP-13	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations.	Personal Data Sub-processing	
DSP-14.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to disclose details to the data owner of any personal or sensitive data access by sub-processors before processing initiation?	Yes	Shared CSP and CSC	Chargebee involves sub-processors as part of the services provided to our customers. We review the technical measures implemented by all our sub-processors in accordance with GDPR, and a mutually agreed Data Processing Addendum is also executed with all the sub-processors. A	Customers could enable or disable third-party integrations after taking into consideration the data transfer to third-party sub-processors. Customers can also review the applicable terms and privacy policy of the third-party provider for the	DSP-14	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing.	Disclosure of Data Sub-processors	
DSP-15.1	Is authorization from data owners obtained, and the associated risk managed, before replicating or using production data in non-production environments?	Yes	CSP-owned	Chargebee does not use customers data for testing / development purposes.	Not Applicable as the control is owned by CSP (Chargebee)	DSP-15	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments.	Limitation of Production Data Use	
DSP-16.1	Do data retention, archiving, and deletion practices follow business requirements, applicable laws, and regulations?	Yes	Shared CSP and CSC	Chargebee retains the customer information only to provide the agreed services and to comply with legal and regulatory commitments. We have established an automated data deletion mechanism in our products	The automated data deletion mechanism in our products and services allowing customers to manage their own data in accordance with their applicable data protection laws/regulations.	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	Data Retention and Deletion	
DSP-17.1	Are processes, procedures, and technical measures defined and implemented to protect sensitive data throughout its lifecycle?	Yes	CSP-owned	Chargebee has implemented and shall maintain appropriate Technical and Organisational Measures (TOMS) to protect customer's data.	Not Applicable as the control is owned by CSP (Chargebee)	DSP-17	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle.	Sensitive Data Protection	
DSP-18.1	Does the CSP have in place, and describe to CSCs, the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations?	Yes	CSP-owned	Refer to our Terms of Service and Data Processing Addendum which is executed with our customers.	Not Applicable as the control is owned by CSP (Chargebee)	DSP-18	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation.	Disclosure Notification	
DSP-18.2	Does the CSP give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation?	Yes	CSP-owned	Refer to our Terms of Service and Data Processing Addendum which is executed with our customers.	Not Applicable as the control is owned by CSP (Chargebee)				
DSP-19.1	Are processes, procedures, and technical measures defined and implemented to specify and document physical data locations, including locales where data is processed or backed up?	Yes	Shared CSP and CSC	Chargebee Billing has Data hosting centres in the US, EU and Australia. Customer has to select the data centre location at the time of signing up / entering into a contract with Chargebee.	For Chargebee Billing, the Customer has to select the data centre location at the time of signing up / entering into a contract with Chargebee.	DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	Data Location	
GRC-01.1	Are information governance program policies and procedures sponsored by organizational leadership established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Chargebee has a well-defined set of Information Security Policies and supporting procedures & guidelines aligned to ISO 27001:2013 standard. All policies and procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)	GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	Governance Program Policy and Procedures	Governance, Risk and Compliance
GRC-01.2	Are the policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
GRC-02.1	Is there an established formal, documented, and leadership-sponsored enterprise risk management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks?	Yes	CSP-owned	Chargebee has defined and implemented a risk management program which sets out the strategy to identify, analyze, evaluate, treat, and review information security risk(s). Risk assessments are performed by the Risk and Compliance team at least annually or at any point in time that a major change takes place from a technology, organization, business, or	Not Applicable as the control is owned by CSP (Chargebee)	GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	Risk Management Program	
GRC-03.1	Are all relevant organizational policies and associated procedures reviewed at least annually, or when a substantial organizational change occurs?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)	GRC-03	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization.	Organizational Policy Reviews	
GRC-04.1	Is an approved exception process mandated by the governance program established and followed whenever a deviation from an established policy occurs?	Yes	CSP-owned	For any exceptions or deviations to the organization's information security policy, the additional risk introduced from the deviation would be analysed and treated by implementing appropriate additional / compensating	Not Applicable as the control is owned by CSP (Chargebee)	GRC-04	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs.	Policy Exception Process	
GRC-05.1	Has an information security program (including programs of all relevant CCM domains) been developed and implemented?	Yes	CSP-owned	Chargebee is committed to ensuring confidentiality, integrity and availability of its information using our Information Security Program. We strive to incorporate Information Security	Not Applicable as the control is owned by CSP (Chargebee)	GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	Information Security Program	
GRC-06.1	Are roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs defined and documented?	Yes	CSP-owned	Chargebee has documented roles and responsibilities for managing the Infosec and improving the Governance program. We have a dedicated Risk and Compliance team, Enterprise Cyber Security team and a Privacy	Not Applicable as the control is owned by CSP (Chargebee)	GRC-06	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs.	Governance Responsibility Model	
GRC-07.1	Are all relevant standards, regulations, legal/contractual, and statutory requirements applicable to your organization identified and documented?	Yes	CSP-owned	Chargebee's Legal team maintains and manages these requirements as applicable.	Not Applicable as the control is owned by CSP (Chargebee)	GRC-07	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization.	Information System Regulatory Mapping	
GRC-08.1	Is contact established and maintained with cloud-related special interest groups and other relevant entities?	Yes	Shared CSP and 3rd-party	We have subscribed to several security/special interest groups, advisories, forums, regulatory newsletters etc.	Not Applicable as the control is owned by CSP (Chargebee)	GRC-08	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context.	Special Interest Groups	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-01.1	Are background verification policies and procedures of all new employees (including but not limited to remote employees, contractors, and third parties) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and 3rd-party	Chargebee has implemented a Background Verification process. All employees are mandatorily required to undergo pre-employment screening, post notification or consensus obtained from the employee. The People Success team undertakes pre-employment screening through third party vendors for all the employees who join Chargebee. The background investigation/screening process	Not Applicable as the control is owned by CSP (Chargebee)			HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually.	Background Screening Policy and Procedures	Human Resources
HRS-01.2	Are background verification policies and procedures designed according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, business requirements, and acceptable risk?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in HRS-01.1	Not Applicable as the control is owned by CSP (Chargebee)						
HRS-01.3	Are background verification policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology and/or regulatory requirements.	Not Applicable as the control is owned by CSP (Chargebee)						
HRS-02.1	Are policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Chargebee has a defined 'Acceptable Usage Policy' which governs the use of organization's assets. Any access to the Chargebee systems and premises are provided only after the employees (including contractors) sign the Acceptable Use Agreements, Code of Conduct and Business Ethics, which forms part of the terms and conditions	Not Applicable as the control is owned by CSP (Chargebee)			HRS-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.	Acceptable Use of Technology Policy and Procedures	
HRS-02.2	Are the policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology and/or regulatory requirements.	Not Applicable as the control is owned by CSP (Chargebee)						
HRS-03.1	Are policies and procedures requiring unattended workspaces to conceal confidential data established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Chargebee has a defined 'Physical and Environmental Security policy' which covers clear desk / clear screen requirements.	Not Applicable as the control is owned by CSP (Chargebee)			HRS-03	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually.	Clean Desk Policy and Procedures	
HRS-03.2	Are policies and procedures requiring unattended workspaces to conceal confidential data reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology and/or regulatory requirements.	Not Applicable as the control is owned by CSP (Chargebee)						
HRS-04.1	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Remote / teleworking is covered as part of the ISMS policies and procedures. All employees are required to follow the guidelines / procedures while working remotely. Enhanced security measures are also implemented to prevent the risk of unauthorized access.	Not Applicable as the control is owned by CSP (Chargebee)			HRS-04	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually.	Remote and Home Working Policy and Procedures	
HRS-04.2	Are policies and procedures to protect information accessed, processed, or stored at remote sites and locations reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)						
HRS-05.1	Are return procedures of organizationally-owned assets by terminated employees established and documented?	Yes	CSP-owned	Chargebee has a well-defined exit process including asset return procedures for terminated employees. Terminated employees will have to return their assets to the IT team	Not Applicable as the control is owned by CSP (Chargebee)			HRS-05	Establish and document procedures for the return of organization-owned assets by terminated employees.	Asset returns	
HRS-06.1	Are procedures outlining the roles and responsibilities concerning changes in employment established, documented, and communicated to all personnel?	Yes	CSP-owned	Chargebee has defined a process for Internal transfers/movement. Associates may request for internal transfer / movement to the existing Department Head, HRBP. The HRBP	Not Applicable as the control is owned by CSP (Chargebee)			HRS-06	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment.	Employment Termination	
HRS-07.1	Are employees required to sign an employment agreement before gaining access to organizational information systems, resources, and assets?	Yes	CSP-owned	As part of the onboarding process, all employees, including contractors, are mandatorily required to sign the contractual agreements as part of terms and conditions in Chargebee.	Not Applicable as the control is owned by CSP (Chargebee)			HRS-07	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets.	Employment Agreement Process	
HRS-08.1	Are provisions and/or terms for adherence to established information governance and security policies included within employment agreements?	Yes	CSP-owned	Please refer to CSP Implementation Description in HRS-07.1	Not Applicable as the control is owned by CSP (Chargebee)			HRS-08	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies.	Employment Agreement Content	
HRS-09.1	Are employee roles and responsibilities relating to information assets and security documented and communicated?	Yes	CSP-owned	Employee Roles and Responsibilities are formally documented and communicated as part of Joining formalities.	Not Applicable as the control is owned by CSP (Chargebee)			HRS-09	Document and communicate roles and responsibilities of employees, as they relate to information assets and security.	Personnel Roles and Responsibilities	
HRS-10.1	Are requirements for non-disclosure/confidentiality agreements reflecting organizational data protection needs and operational details identified, documented, and reviewed at planned intervals?	Yes	CSP-owned	Chargebee's Legal team reviews NDA/Agreements at planned intervals to ensure appropriateness.	Not Applicable as the control is owned by CSP (Chargebee)			HRS-10	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details.	Non-Disclosure Agreements	
HRS-11.1	Is a security awareness training program for all employees of the organization established, documented, approved, communicated, applied, evaluated and maintained?	Yes	CSP-owned	Chargebee has an on-going Information Security Awareness Program. All Employees including Interns and contractors, are mandatorily required to attend the training as part of the new hire	Not Applicable as the control is owned by CSP (Chargebee)			HRS-11	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates.	Security Awareness Training	
HRS-11.2	Are regular security awareness training updates provided?	Yes	CSP-owned	Please refer to CSP Implementation Description in HRS-11.1	Not Applicable as the control is owned by CSP (Chargebee)						
HRS-12.1	Are all employees granted access to sensitive organizational and personal data provided with appropriate security awareness training?	Yes	CSP-owned	Security awareness trainings are provided to all employees periodically. Not all employees granted access to sensitive/personal data. Access to Chargebee information systems are provided only on a need basis as per the business requirements upon authorization and follows least privilege	Not Applicable as the control is owned by CSP (Chargebee)			HRS-12	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Personal and Sensitive Data Awareness and Training	
HRS-12.2	Are all employees granted access to sensitive organizational and personal data provided with regular updates in procedures, processes, and policies relating to their professional function?	Yes	CSP-owned	Please refer to CSP Implementation Description in HRS-12.1	Not Applicable as the control is owned by CSP (Chargebee)						

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
HRS-13.1	Are employees notified of their roles and responsibilities to maintain awareness and compliance with established policies, procedures, and applicable legal, statutory, or regulatory compliance obligations?	Yes	CSP-owned	Please refer to CSP Implementation Description in HRS-11.1	Not Applicable as the control is owned by CSP (Chargebee)	HRS-13	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.	Compliance User Responsibility	
IAM-01.1	Are identity and access management policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	Chargebee has a clearly defined 'Logical Access Control Policy' and 'Logical Access Control Procedure' as part of our ISMS framework which includes aspects such as access provisioning, maintaining, revoking and [illegible]	Access to merchant's Chargebee site (provisioning, deprovisioning and user access reviews) are managed by the admin/owner/site user from the merchant's end.	IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually.	Identity and Access Management Policy and Procedures	
IAM-01.2	Are identity and access management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
IAM-02.1	Are strong password policies and procedures established, documented, approved, communicated, implemented, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	Chargebee has defined a strong password policy in line with industry best practices which includes the following parameters: Password Length, Password Complexity, Password Age and Password History	Merchants may choose to configure SSO / MFA based on their requirement to further enhance access security for their site/account.	IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	Strong Password Policy and Procedures	
IAM-02.2	Are strong password policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
IAM-03.1	Is system identity information and levels of access managed, stored, and reviewed?	Yes	Shared CSP and CSC	User's access inventory is maintained by Chargebee and reviewed periodically.	Chargebee products have an in-built authentication module where it provides the ability for customers to define user names and assign access roles (both standard/custom).	IAM-03	Manage, store, and review the information of system identities, and level of access.	Identity Inventory	
IAM-04.1	Is the separation of duties principle employed when implementing information system access?	Yes	Shared CSP and CSC	Chargebee has both environment level and access level segregation between the development, staging, and production environments. User privileges are provided based on roles	Please refer to CSC Responsibilities in IAM-01.1 & IAM-03.1	IAM-04	Employ the separation of duties principle when implementing information system access.	Separation of Duties	
IAM-05.1	Is the least privilege principle employed when implementing information system access?	Yes	Shared CSP and CSC	Access to Chargebee's information systems is provided only on an as-needed basis as per the business requirements upon authorization and follows least privilege principle.	Please refer to CSC Responsibilities in IAM-01.1 & IAM-03.1	IAM-05	Employ the least privilege principle when implementing information system access.	Least Privilege	
IAM-06.1	Is a user access provisioning process defined and implemented which authorizes, records, and communicates data and assets access changes?	Yes	Shared CSP and CSC	Please refer to CSP Implementation Description in IAM-01.1	Please refer to CSC Responsibilities in IAM-01.1 & IAM-03.1	IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	User Access Provisioning	
IAM-07.1	Is a process in place to de-provision or modify the access, in a timely manner, of movers / leavers or system identity changes, to effectively adopt and communicate identity and access management policies?	Yes	Shared CSP and CSC	Please refer to CSP Implementation Description in IAM-01.1	Please refer to CSC Responsibilities in IAM-01.1 & IAM-03.1	IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies.	User Access Changes and Revocation	
IAM-08.1	Are reviews and revalidation of user access for least privilege and separation of duties completed with a frequency commensurate with organizational risk tolerance?	Yes	Shared CSP and CSC	User access review is performed by the Risk and Compliance Team in conjunction with the relevant department on a quarterly basis to ensure only authorized users have access rights to services, systems, and [illegible]	Please refer to CSC Responsibilities in IAM-01.1 & IAM-03.1	IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	User Access Review	
IAM-09.1	Are processes, procedures, and technical measures for the segregation of privileged access roles defined, implemented, and evaluated such that administrative data access, encryption, key management capabilities, and logging capabilities are distinct and separate?	Yes	Shared CSP and CSC	Administrative privileges are restricted only to authorized users and managed through role-based access controls on all information systems. Such access are provided based on appropriate approvals and for the agreed timeframe. Two-factor authentication is enabled for all privileged access to Chargebee's information system.	Please refer to CSC Responsibilities in IAM-01.1 & IAM-03.1	IAM-09	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated.	Segregation of Privileged Access Roles	Identity & Access Management
IAM-10.1	Is an access process defined and implemented to ensure privileged access roles and rights are granted for a limited period?	Yes	Shared CSP and CSC	Please refer to CSP Implementation Description in IAM-09.1	Please refer to CSC Responsibilities in IAM-01.1 & IAM-03.1	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access.	Management of Privileged Access Roles	
IAM-10.2	Are procedures implemented to prevent the culmination of segregated privileged access?	Yes	CSP-owned	Segregation of environments by implementing dedicated AWS accounts for development, staging and production. Within these environments, Chargebee has designed dedicated groups to ensure segregated access [illegible]	Please refer to CSC Responsibilities in IAM-01.1 & IAM-03.1				
IAM-11.1	Are processes and procedures for customers to participate, where applicable, in granting access for agreed, high risk as (defined by the organizational risk assessment) privileged access roles defined, implemented and evaluated?	Yes	Shared CSP and CSC	Being a SAAS product, Chargebee is multi-tenant service provider and provides access to its customers to the front end applications for the respective customer owned sites. Customers are allowed to manage their accesses as part of account management for their dedicated	Please refer to CSC Responsibilities in IAM-01.1 & IAM-03.1	IAM-11	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles.	CSCs Approval for Agreed Privileged Access Roles	
IAM-12.1	Are processes, procedures, and technical measures to ensure the logging infrastructure is "read-only" for all with write access (including privileged access roles) defined, implemented, and evaluated?	Yes	CSP-owned	Yes, Audit and event logs are protected and are "read-only" and access to these logs are restricted only to the authorised team.	Not Applicable as the control is owned by CSP (Chargebee)	IAM-12	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures.	Safeguard Logs Integrity	
IAM-12.2	Is the ability to disable the "read-only" configuration of logging infrastructure controlled through a procedure that ensures the segregation of duties and break glass procedures?	Yes	CSP-owned	Only authorised administrators can make such change and the same is logged and monitored.	Not Applicable as the control is owned by CSP (Chargebee)				
IAM-13.1	Are processes, procedures, and technical measures that ensure users are identifiable through unique identification (or can associate individuals with user identification usage) defined, implemented, and evaluated?	Yes	CSP-owned	Users are provided with unique identification.	Not Applicable as the control is owned by CSP (Chargebee)	IAM-13	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs.	Uniquely Identifiable Users	
IAM-14.1	Are processes, procedures, and technical measures for authenticating access to systems, application, and data assets including multifactor authentication for a least-privileged user and sensitive data access defined, implemented, and evaluated?	Yes	Shared CSP and CSC	Two-factor authentication is enabled for all privileged access / critical systems in Chargebee's environment.	Please refer to CSC Responsibilities in IAM-02.1	IAM-14	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	Strong Authentication	
IAM-14.2	Are digital certificates or alternatives that achieve an equivalent security level for system identities adopted?	Yes	CSP-owned	For internal tools, Chargebee uses OKTA as IDP solution which is MFA enabled.	Please refer to CSC Responsibilities in IAM-02.1				
IAM-15.1	Are processes, procedures, and technical measures for the secure management of passwords defined, implemented, and evaluated?	Yes	CSP-owned	Passwords are salted and hashed using bcrypt when stored on database.	Not Applicable as the control is owned by CSP (Chargebee)	IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	Passwords Management	

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IAM-16.1	Are processes, procedures, and technical measures to verify access to data and system functions authorized, defined, implemented, and evaluated?	Yes	Shared CSP and CSC	Access to Chargebee's information systems is provided only on an as-needed basis as per the business requirements upon authorization and follows least privilege principle. Two-	Please refer to CSC Responsibilities in IAM-03.1			IAM-16	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized.	Authorization Mechanisms	
IPY-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for communications between application services (e.g., APIs)?	Yes	Shared CSP and CSC	Chargebee provides standard REST-APIs that helps the customers to programmatically interface Chargebee products with their solutions. More details on the API usage is available on our API helpdocs . Chargebee also has a marketplace which offers third-party integrations.	Merchants can follow the guidelines provided in the API helpdocs and implement it as per their requirement.			IPY-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually.	Interoperability and Portability Policy and Procedures	Interoperability & Portability
IPY-01.2	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information processing interoperability?	Yes	Shared CSP and CSC	Please refer to CSP Implementation Description in IPY-01.1	Please refer to CSC Responsibilities in IPY-01.1						
IPY-01.3	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for application development portability?	Yes	CSP-owned	Application portability is considered and implemented at the design stage of our Software development lifecycle.	Not Applicable as the control is owned by CSP (Chargebee)						
IPY-01.4	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for information/data exchange, usage, portability, integrity, and persistence?	Yes	Shared CSP and CSC	Please refer to CSP Implementation Description in IPY-01.1	Please refer to CSC Responsibilities in IPY-01.1						
IPY-01.5	Are interoperability and portability policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	These are reviewed on a need-basis.	Not Applicable as the control is owned by CSP (Chargebee)						
IPY-02.1	Are CSCs able to programmatically retrieve their data via an application interface(s) to enable interoperability and portability?	Yes	Shared CSP and CSC	Please refer to CSP Implementation Description in IPY-01.1	Please refer to CSC Responsibilities in IPY-01.1			IPY-02	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability.	Application Interface Availability	
IPY-03.1	Are cryptographically secure and standardized network protocols implemented for the management, import, and export of data?	Yes	CSP-owned	API calls to Chargebee services are encrypted using industry standard protocols.	Not Applicable as the control is owned by CSP (Chargebee)			IPY-03	Implement cryptographically secure and standardized network protocols for the management, import and export of data.	Secure Interoperability and Portability Management	
IPY-04.1	Do agreements include provisions specifying CSC data access upon contract termination, and have the following? a. Data format b. Duration data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Yes	Shared CSP and CSC	Chargebee retains the customer information only to provide the agreed services and to comply with legal and regulatory commitments. We have established an automated data deletion mechanism in our products and services allowing customers to manage their own data. We will clear/obfuscate the customer's Personally Identifiable Information (PII)	The automated data deletion mechanism in our products and services allowing customers to manage their own data in accordance with their applicable data protection laws/regulations. Customers are responsible for data export before termination of services.			IPY-04	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy	Data Portability Contractual Obligations	
IVS-01.1	Are infrastructure and virtualization security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Chargebee has a well-defined set of Information Security Policies and supporting procedures & guidelines aligned to ISO 27001:2013 standard. All policies and procedures are reviewed at least annually or when	Not Applicable as the control is owned by CSP (Chargebee)			IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	Infrastructure and Virtualization Security Policy and Procedures	Infrastructure & Virtualization Security
IVS-01.2	Are infrastructure and virtualization security policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)						
IVS-02.1	Is resource availability, quality, and capacity planned and monitored in a way that delivers required system performance, as determined by the business?	Yes	CSP-owned	Chargebee has defined and documented a Capacity Management process to ensure utilization of resources is being monitored, tuned and projections made on future capacity requirements to ensure the	Not Applicable as the control is owned by CSP (Chargebee)			IVS-02	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business.	Capacity and Resource Planning	
IVS-03.1	Are communications between environments monitored?	Yes	CSP-owned	Chargebee has also established a 24x7 CPE (Cloud Production Engineering) and SOC (Security Operations Center) team that monitors various security events and patterns.	Not Applicable as the control is owned by CSP (Chargebee)			IVS-03	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls.	Network Security	
IVS-03.2	Are communications between environments encrypted?	Yes	CSP-owned	All communications to the Chargebee platform are through an encrypted tunnel using TLS 1.2 with AES encryption ranging from 128-bit and 256-bit for secure connections of data transfer over unsecure Internet.	Not Applicable as the control is owned by CSP (Chargebee)						
IVS-03.3	Are communications between environments restricted to only authenticated and authorized connections, as justified by the business?	Yes	CSP-owned	Chargebee has implemented VPN solution to connect to Chargebee environments where access is provisioned through least privilege principle. Further, Chargebee has configured Security groups and NACL which strictly segregate the environments within Chargebee's infrastructure.	Not Applicable as the control is owned by CSP (Chargebee)						
IVS-03.4	Are network configurations reviewed at least annually?	Yes	CSP-owned	Chargebee uses AWS for cloud infrastructure. Network configuration are reviewed on a need basis or whenever there is a major change.	Not Applicable as the control is owned by CSP (Chargebee)						
IVS-03.5	Are network configurations supported by the documented justification of all allowed services, protocols, ports, and compensating controls?	Yes	CSP-owned	Chargebee's Cloud Infrastructure team maintains the documentation of our network architecture. Only the required and secure services, protocols and ports are allowed.	Not Applicable as the control is owned by CSP (Chargebee)						

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
IVS-04.1	Is every host and guest OS, hypervisor, or infrastructure control plane hardened (according to their respective best practices) and supported by technical controls as part of a security baseline?	Yes	CSP-owned	Vulnerability scanning and remediation practices are regularly reviewed as part of Chargebee's continued compliance with PCI DSS and ISO 27001.	Not Applicable as the control is owned by CSP (Chargebee)	IVS-04	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	OS Hardening and Base Controls	
IVS-05.1	Are production and non-production environments separated?	Yes	CSP-owned	Chargebee has environment level segregation between the development, staging and production environments. Separate VPCs and Amazon accounts	Not Applicable as the control is owned by CSP (Chargebee)	IVS-05	Separate production and non-production environments.	Production and Non-Production Environments	
IVS-06.1	Are applications and infrastructures designed, developed, deployed, and configured such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented, segregated, monitored, and restricted from other tenants?	Yes	CSP-owned	Chargebee uses a multi-tenant data model to host all its applications. Our infrastructure and platform are hosted in segregated VPCs for increased security and manageability. Chargebee uses Amazon's RDS for the storage of customer data. Customer data is logically segregated from other clients through database keys. No customer	Not Applicable as the control is owned by CSP (Chargebee)	IVS-06	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.	Segmentation and Segregation	
IVS-07.1	Are secure and encrypted communication channels including only up-to-date and approved protocols used when migrating servers, services, applications, or data to cloud environments?	Yes	CSP-owned	All communications to the Chargebee platform are through an encrypted tunnel using TLS 1.2 with AES encryption ranging from 128-bit and 256-bit for secure connections of data transfer over unsecure Internet.	Not Applicable as the control is owned by CSP (Chargebee)	IVS-07	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols.	Migration to Cloud Environments	
IVS-08.1	Are high-risk environments identified and documented?	Yes	CSP-owned	Chargebee has performed and documented detailed assessments to identify internal environments based on risk level, compliance and regulatory	Not Applicable as the control is owned by CSP (Chargebee)	IVS-08	Identify and document high-risk environments.	Network Architecture Documentation	
IVS-09.1	Are processes, procedures, and defense-in-depth techniques defined, implemented, and evaluated for protection, detection, and timely response to network-based attacks?	Yes	CSP-owned	Chargebee's application can be reached only through HTTPS. Application traffic is allowed only through Load balancer which is integrated with Web Application Firewall to help us protect against security and availability risks such as DDoS. Also, our backend systems that	Not Applicable as the control is owned by CSP (Chargebee)	IVS-09	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks.	Network Defense	
LOG-01.1	Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Chargebee has a well-defined set of Information Security Policies and supporting procedures & guidelines aligned to ISO 27001:2013 standard. All policies and procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory	Not Applicable as the control is owned by CSP (Chargebee)	LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	Logging and Monitoring Policy and Procedures	
LOG-01.2	Are policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
LOG-02.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to ensure audit log security and retention?	Yes	CSP-owned	Chargebee has developed and implemented a comprehensive Audit logging and Monitoring program for securing its information systems. Audit trail files are retained and are available	Not Applicable as the control is owned by CSP (Chargebee)	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	Audit Logs Protection	
LOG-03.1	Are security-related events identified and monitored within applications and the underlying infrastructure?	Yes	CSP-owned	All application, servers and database activities are logged and monitored through SIEM tool. Event Correlation rules are implemented on the SIEM tool and are configured to generate alerts when the traffic patterns match the implemented rules for any potential security event. These alerts are	Not Applicable as the control is owned by CSP (Chargebee)	LOG-03	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics.	Security Monitoring and Alerting	
LOG-03.2	Is a system defined and implemented to generate alerts to responsible stakeholders based on security events and their corresponding metrics?	Yes	CSP-owned	Chargebee has implemented SNORT, a Host-based Intrusion Detection system to monitor and log alerts. All SNORT alerts are forwarded to the SIEM tool and monitored on a 24x7 basis. Chargebee also utilizes monitoring tools with automated alert mechanisms which triggers alerts to	Not Applicable as the control is owned by CSP (Chargebee)				
LOG-04.1	Is access to audit logs restricted to authorized personnel, and are records maintained to provide unique access accountability?	Yes	CSP-owned	Access to Audit trails and logs are restricted to authorized personnel based on roles and responsibilities. Segregation of duties is implemented to restrict the system administrators	Not Applicable as the control is owned by CSP (Chargebee)	LOG-04	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability.	Audit Logs Access and Accountability	Logging and Monitoring
LOG-05.1	Are security audit logs monitored to detect activity outside of typical or expected patterns?	Yes	CSP-owned	All application, servers and database activities are logged and monitored through SIEM tool. Event Correlation rules are implemented on the SIEM tool and are configured to generate alerts when the traffic patterns match	Not Applicable as the control is owned by CSP (Chargebee)	LOG-05	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies.	Audit Logs Monitoring and Response	
LOG-05.2	Is a process established and followed to review and take appropriate and timely actions on detected anomalies?	Yes	CSP-owned	The CPE and SOC team monitor/reviews these alerts and share with the relevant owners for appropriate actions.	Not Applicable as the control is owned by CSP (Chargebee)				
LOG-06.1	Is a reliable time source being used across all relevant information processing systems?	Yes	CSP-owned	Chargebee is hosted in AWS that uses Amazon Time Sync Service, a time synchronization service delivered over Network Time Protocol (NTP).	Not Applicable as the control is owned by CSP (Chargebee)	LOG-06	Use a reliable time source across all relevant information processing systems.	Clock Synchronization	
LOG-07.1	Are logging requirements for information meta/data system events established, documented, and implemented?	Yes	CSP-owned	Chargebee uses logging and monitoring tools to log and monitor application usage metadata and traffic access logs. These logs are used to ensure and enhance service delivery and also aid in security event monitoring.	Not Applicable as the control is owned by CSP (Chargebee)	LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	Logging Scope	
LOG-07.2	Is the scope reviewed and updated at least annually, or whenever there is a change in the threat environment?	Yes	CSP-owned	The scope is reviewed on a need-basis.	Not Applicable as the control is owned by CSP (Chargebee)				
LOG-08.1	Are audit records generated, and do they contain relevant security information?	Yes	CSP-owned	Logs contain relevant security information.	Not Applicable as the control is owned by CSP (Chargebee)	LOG-08	Generate audit records containing relevant security information.	Log Records	
LOG-09.1	Does the information system protect audit records from unauthorized access, modification, and deletion?	Yes	CSP-owned	Access to Audit trails and logs are restricted to authorized personnel based on roles and responsibilities. Segregation of duties is implemented to restrict the system administrators	Not Applicable as the control is owned by CSP (Chargebee)	LOG-09	The information system protects audit records from unauthorized access, modification, and deletion.	Log Protection	
LOG-10.1	Are monitoring and internal reporting capabilities established to report on cryptographic operations, encryption, and key management policies, processes, procedures, and controls?	Yes	CSP-owned	Chargebee has a Cryptography and Key management policy and procedure to protect the confidentiality, authenticity, or integrity of information through encryption. We use the AWS Managed Keys - KMS for encryption.	Not Applicable as the control is owned by CSP (Chargebee)	LOG-10	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls.	Encryption Monitoring and Reporting	
LOG-11.1	Are key lifecycle management events logged and monitored to enable auditing and reporting on cryptographic keys' usage?	Yes	CSP-owned	Such events are logged and maintained.	Not Applicable as the control is owned by CSP (Chargebee)	LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	Transaction/Activity Logging	
LOG-12.1	Is physical access logged and monitored using an auditable access control system?	Yes	Shared CSP and 3rd-party	Physical security at Chargebee: Access is restricted to authorized employees and authentication such as access card and/or biometric screening is required to gain access to	Not Applicable as the control is owned by 3rd Party(AWS)	LOG-12	Monitor and log physical access using an auditable access control system.	Access Control Logs	
LOG-13.1	Are processes and technical measures for reporting monitoring system anomalies and failures defined, implemented, and evaluated?	Yes	CSP-owned	Please refer to CSP Implementation Description in LOG-03.1 and LOG-03.2	Not Applicable as the control is owned by CSP (Chargebee)	LOG-13	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party.	Failures and Anomalies Reporting	
LOG-13.2	Are accountable parties immediately notified about anomalies and failures?	Yes	CSP-owned	Please refer to CSP Implementation Description in LOG-03.1 and LOG-03.2	Not Applicable as the control is owned by CSP (Chargebee)				

CAIQ™ **CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2**

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
SEF-01.1	Are policies and procedures for security incident management, e-discovery, and cloud forensics established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Chargebee has established a formal security incident management procedure which defines how an information security incident is reported, handled, responded to, and recorded. Information security	Not Applicable as the control is owned by CSP (Chargebee)	SEF-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually.	Security Incident Management Policy and Procedures	Security Incident Management, E-Discovery, & Cloud Forensics
SEF-01.2	Are policies and procedures reviewed and updated annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
SEF-02.1	Are policies and procedures for timely management of security incidents established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Please refer to CSP Implementation Description in SEF-01.1	Not Applicable as the control is owned by CSP (Chargebee)	SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually.	Service Management Policy and Procedures	
SEF-02.2	Are policies and procedures for timely management of security incidents reviewed and updated at least annually?	Yes	CSP-owned	Please refer to CSP Implementation Description in SEF-01.2	Not Applicable as the control is owned by CSP (Chargebee)				
SEF-03.1	Is a security incident response plan that includes relevant internal departments, impacted CSCs, and other business-critical relationships (such as supply-chain) established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Please refer to CSP Implementation Description in SEF-01.1	Not Applicable as the control is owned by CSP (Chargebee)	SEF-03	'Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.'	Incident Response Plans	
SEF-04.1	Is the security incident response plan tested and updated for effectiveness, as necessary, at planned intervals or upon significant organizational or environmental changes?	Yes	CSP-owned	The incident response plan is tested on a periodic basis and the same is periodically reviewed as part of internal audit. This is also audited as part of ISO 27001 and SOC 2 Type 2 attestation.	Not Applicable as the control is owned by CSP (Chargebee)	SEF-04	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness.	Incident Response Testing	
SEF-05.1	Are information security incident metrics established and monitored?	Yes	CSP-owned	The information security incident metrics are established and monitored centrally by the MIM team.	Not Applicable as the control is owned by CSP (Chargebee)	SEF-05	Establish and monitor information security incident metrics.	Incident Response Metrics	
SEF-06.1	Are processes, procedures, and technical measures supporting business processes to triage security-related events defined, implemented, and evaluated?	Yes	CSP-owned	Chargebee has a dedicated Enterprise Cyber Security (ECS) team which has established processes and procedures to triage security events as part of the Vulnerability Management Process.	Not Applicable as the control is owned by CSP (Chargebee)	SEF-06	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events.	Event Triage Processes	
SEF-07.1	Are processes, procedures, and technical measures for security breach notifications defined and implemented?	Yes	CSP-owned	All suspected personal data breaches are raised as tickets within the service desk tool with a detailed description. Breaches logged are reviewed against existing records to ascertain patterns or re-occurrences. A full investigation is conducted by the Risk & Compliance and ECS team and the results are	Not Applicable as the control is owned by CSP (Chargebee)	SEF-07	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	Security Breach Notification	
SEF-07.2	Are security breaches and assumed security breaches reported (including any relevant supply chain breaches) as per applicable SLAs, laws, and regulations?	Yes	CSP-owned	Chargebee shall, to the extent permitted by law, notify Customer of any Personal Data Breach no later than seventy-two (72) hours from the time Chargebee becomes aware of the Personal Data Breach.	Not Applicable as the control is owned by CSP (Chargebee)				
SEF-08.1	Are points of contact maintained for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities?	Yes	CSP-owned	We maintain appropriate contacts with legal authorities, where required by applicable regulatory bodies.	Not Applicable as the control is owned by CSP (Chargebee)	SEF-08	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities.	Points of Contact Maintenance	
STA-01.1	Are policies and procedures implementing the shared security responsibility model (SSRM) within the organization established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	Shared CSP and CSC	Responsibilities are defined and agreed as part of the Contractual agreements. Please refer to our Terms of Service - and Data processing addendum for more details. Chargebee has also published a PCI Responsibility Matrix specifically for the scope of PCI highlighting the responsibilities of Chargebee and our	Responsibilities are defined and agreed as part of the Contractual agreements. Please refer to our Terms of Service - and Data processing addendum for more details. Chargebee has also published a PCI Responsibility Matrix specifically for the scope of PCI highlighting the responsibilities of Chargebee and our	STA-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually.	SSRM Policy and Procedures	Supply Chain Management, Transparency, and Accountability
STA-01.2	Are the policies and procedures that apply the SSRM reviewed and updated annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
STA-02.1	Is the SSRM applied, documented, implemented, and managed throughout the supply chain for the cloud service offering?	Yes	Shared CSP and 3rd-party	Chargebee has a comprehensive Vendor Management Program in place to evaluate, select and monitor vendors in order to minimize the risks associated with third party vendors. Suppliers are also required to complete	Not Applicable as the control is owned by CSP (Chargebee)	STA-02	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering.	SSRM Supply Chain	
STA-03.1	Is the CSC given SSRM guidance detailing information about SSRM applicability throughout the supply chain?	Yes	Shared CSP and CSC	Responsibilities are defined and agreed as part of the Contractual agreements. Please refer to our Terms of Service - and Data processing addendum for more details.	Responsibilities are defined and agreed as part of the Contractual agreements. Please refer to our Terms of Service - and Data processing addendum for more details.	STA-03	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain.	SSRM Guidance	
STA-04.1	Is the shared ownership and applicability of all CSA CCM controls delineated according to the SSRM for the cloud service offering?	Yes	Shared CSP and CSC	Responsibilities are defined and agreed as part of the Contractual agreements. Please refer to our Terms of Service - and Data processing addendum for more details.	Responsibilities are defined and agreed as part of the Contractual agreements. Please refer to our Terms of Service - and Data processing addendum for more details.	STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	SSRM Control Ownership	
STA-05.1	Is SSRM documentation for all cloud services the organization uses reviewed and validated?	Yes	CSP-owned	Reviewed as and when applicable.	Not Applicable as the control is owned by CSP (Chargebee)	STA-05	Review and validate SSRM documentation for all cloud services offerings the organization uses.	SSRM Documentation Review	
STA-06.1	Are the portions of the SSRM the organization is responsible for implemented, operated, audited, or assessed?	Yes	CSP-owned	Chargebee undergoes an external audit as part of its ISO 27001 certification and SOC 2 Type II attestation engagement performed by an external independent global audit	Not Applicable as the control is owned by CSP (Chargebee)	STA-06	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for.	SSRM Control Implementation	
STA-07.1	Is an inventory of all supply chain relationships developed and maintained?	Yes	CSP-owned	Chargebee and its group companies use sub-processors to assist them in connection with the Services (as described in the Terms of service).	Not Applicable as the control is owned by CSP (Chargebee)	STA-07	Develop and maintain an inventory of all supply chain relationships.	Supply Chain Inventory	
STA-08.1	Are risk factors associated with all organizations within the supply chain periodically reviewed by CSPs?	Yes	CSP-owned	Suppliers' performance to the defined service level agreements will be monitored continuously and periodic reviews are conducted as and when necessary. In addition to an annual	Not Applicable as the control is owned by CSP (Chargebee)	STA-08	CSPs periodically review risk factors associated with all organizations within their supply chain.	Supply Chain Risk Management	
STA-09.1	Do service agreements between CSPs and CSCs (tenants) incorporate at least the following mutually agreed upon provisions and/or terms? • Scope, characteristics, and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third-party assessment • Service termination • Interoperability and portability requirements • Data privacy	Yes	Shared CSP and CSC	Please refer to our Terms of Service - and Data processing addendum.	This is covered as part of the contractual documents.	STA-09	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy	Primary Service and Contractual Agreement	
STA-10.1	Are supply chain agreements between CSPs and CSCs reviewed at least annually?	Yes	Shared CSP and CSC	Our Online terms of services are reviewed and updated as and when there are major changes. However, the custom agreements between CSP and	Custom agreements between CSP and CSC's are reviewed during renewal or as agreed by both the parties.	STA-10	Review supply chain agreements between CSPs and CSCs at least annually.	Supply Chain Agreement Review	

CAIQ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
STA-11.1	Is there a process for conducting internal assessments at least annually to confirm the conformance and effectiveness of standards, policies, procedures, and SLA activities?	Yes	CSP-owned	Suppliers' performance to the defined service level agreements will be monitored continuously and periodic reviews are conducted as and when necessary. In addition to an annual review, supplier information security	Not Applicable as the control is owned by CSP (Chargebee)	STA-11	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually.	Internal Compliance Testing	
STA-12.1	Are policies that require all supply chain CSPs to comply with information security, confidentiality, access control, privacy, audit, personnel policy, and service level requirements and standards implemented?	Yes	Shared CSP and 3rd-party	Contractual Agreements and a Data Processing Addendum (as applicable) are executed with our third party suppliers and sub-processors, which provides contractual commitments to our compliance with applicable Laws, regulations and requirements.	Not Applicable as the control is owned by CSP (Chargebee)	STA-12	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards.	Supply Chain Service Agreement Compliance	
STA-13.1	Are supply chain partner IT governance policies and procedures reviewed periodically?	Yes	Shared CSP and 3rd-party	Supplier information security assessments are conducted on a regular basis (as necessary) for business critical tools/service providers to ensure that they remain current. The	Not Applicable as the control is owned by CSP (Chargebee)	STA-13	Periodically review the organization's supply chain partners' IT governance policies and procedures.	Supply Chain Governance Review	
STA-14.1	Is a process to conduct periodic security assessments for all supply chain organizations defined and implemented?	Yes	Shared CSP and 3rd-party	Please refer to CSP Implementation Description in STA-13.1	Not Applicable as the control is owned by CSP (Chargebee)	STA-14	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain.	Supply Chain Data Security Assessment	
TVM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to identify, report, and prioritize the remediation of vulnerabilities to protect systems against vulnerability exploitation?	Yes	CSP-owned	Chargebee has a defined Vulnerability Management Policy and Procedure to provide a common set of methodologies and requirements to standardize vulnerability scans on Chargebee Servers and networking infrastructure and to identify and remediate vulnerabilities across all	Not Applicable as the control is owned by CSP (Chargebee)	TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	Threat and Vulnerability Management Policy and Procedures	Threat & Vulnerability Management
TVM-01.2	Are threat and vulnerability management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
TVM-02.1	Are policies and procedures to protect against malware on managed assets established, documented, approved, communicated, applied, evaluated, and maintained?	Yes	CSP-owned	Chargebee has implemented an anti-virus and malware protection policy and procedure as part of the Information Security Policies aligned to ISO 27001:2013 standard.	Not Applicable as the control is owned by CSP (Chargebee)	TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	Malware Protection Policy and Procedures	
TVM-02.2	Are asset management and malware protection policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Policies and Procedures are reviewed at least annually or when there is a significant change in the business, technology, regulatory and/or product enhancement.	Not Applicable as the control is owned by CSP (Chargebee)				
TVM-03.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable scheduled and emergency responses to vulnerability identifications (based on the identified risk)?	Yes	CSP-owned	Identified vulnerabilities are tracked, prioritized based on urgency, and assigned to relevant owners as a ticket until resolved.	Not Applicable as the control is owned by CSP (Chargebee)	TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	Vulnerability Remediation Schedule	
TVM-04.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to update detection tools, threat signatures, and compromise indicators weekly (or more frequent) basis?	Yes	CSP-owned	Chargebee uses Managed Services where automatic download and application of signature updates occur as per Vendor schedule from the vendor's virus definition site.	Not Applicable as the control is owned by CSP (Chargebee)	TVM-04	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis.	Detection Updates	
TVM-05.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to identify updates for applications that use third-party or open-source libraries (according to the organization's vulnerability management policy)?	Yes	Shared CSP and 3rd-party	Chargebee's Vulnerability Management program has capability to identify updates for applications that use third-party or open-source libraries using Source Code Composition Analysis tools.	Not Applicable as the control is owned by CSP (Chargebee)	TVM-05	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy.	External Library Vulnerabilities	
TVM-06.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for periodic, independent, third-party penetration testing?	Yes	Shared CSP and 3rd-party	Penetration testing is performed by an outsourced accredited supplier covering Chargebee applications and supporting infrastructure on an annual basis.	Not Applicable as the control is owned by CSP (Chargebee)	TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	Penetration Testing	
TVM-07.1	Are processes, procedures, and technical measures defined, implemented, and evaluated for vulnerability detection on organizationally managed assets at least monthly?	Yes	Shared CSP and 3rd-party	Chargebee has defined and documented a formal Vulnerability Management Policy and Procedure to provide a common set of methodologies and requirements to standardize vulnerability scans on Chargebee Servers and networking infrastructure and to identify and	Not Applicable as the control is owned by CSP (Chargebee)	TVM-07	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly.	Vulnerability Identification	
TVM-08.1	Is vulnerability remediation prioritized using a risk-based model from an industry-recognized framework?	Yes	CSP-owned	Once we identify a vulnerability requiring remediation, it is logged, prioritized according to the severity, and assigned to an owner. CVSS 3.0 framework is used as the basis of	Not Applicable as the control is owned by CSP (Chargebee)	TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	Vulnerability Prioritization	
TVM-09.1	Is a process defined and implemented to track and report vulnerability identification and remediation activities that include stakeholder notification?	Yes	CSP-owned	Please refer to CSP Implementation Description in TVM-08.1	Not Applicable as the control is owned by CSP (Chargebee)	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	Vulnerability Management Reporting	
TVM-10.1	Are metrics for vulnerability identification and remediation established, monitored, and reported at defined intervals?	Yes	CSP-owned	On a regular basis, Chargebee tracks and monitors critical metrics driving the Vulnerability management process.	Not Applicable as the control is owned by CSP (Chargebee)	TVM-10	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals.	Vulnerability Management Metrics	
UEM-01.1	Are policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained for all endpoints?	Yes	CSP-owned	Chargebee has a defined IT Asset Management policy and procedure inline with ISO 27001 standards. All policies and procedures are reviewed at least annually or when there is a significant change in the business,	Not Applicable as the control is owned by CSP (Chargebee)	UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	Endpoint Devices Policy and Procedures	Universal Endpoint Management
UEM-01.2	Are universal endpoint management policies and procedures reviewed and updated at least annually?	Yes	CSP-owned	Please refer to CSP Implementation Description in UEM-01.1	Not Applicable as the control is owned by CSP (Chargebee)				
UEM-02.1	Is there a defined, documented, applicable and evaluated list containing approved services, applications, and the sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data?	Yes	CSP-owned	Chargebee has a defined 'Acceptable Usage Policy' which governs the use of organization's assets. Any access to the Chargebee systems and premises are provided only after the employees (including contractors) sign the Acceptable Use Agreements, Code of Conduct and Business Ethics, which forms part of the terms and conditions	Not Applicable as the control is owned by CSP (Chargebee)	UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	Application and Service Approval	
UEM-03.1	Is a process defined and implemented to validate endpoint device compatibility with operating systems and applications?	Yes	CSP-owned	Chargebee has established Asset management policy in line with ISO 27001 standards which includes compatibility and validation checks for endpoints.	Not Applicable as the control is owned by CSP (Chargebee)	UEM-03	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications.	Compatibility	
UEM-04.1	Is an inventory of all endpoints used and maintained to store and access company data?	Yes	CSP-owned	All the assets are clearly identified and an inventory of all assets is drawn up and maintained on an ongoing basis in the IT asset management tool. Information assets are broadly grouped into following major categories:	Not Applicable as the control is owned by CSP (Chargebee)	UEM-04	Maintain an inventory of all endpoints used to store and access company data.	Endpoint Inventory	
UEM-05.1	Are processes, procedures, and technical measures defined, implemented and evaluated, to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data?	Yes	CSP-owned	IT team is responsible for managing corporate computing devices including laptops/endpoints, business applications, org-wide tools, and employee and contractor identities. SSO and MFA are configured as applicable to enhance the security level of such assets. All endpoints are	Not Applicable as the control is owned by CSP (Chargebee)	UEM-05	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data.	Endpoint Management	
UEM-06.1	Are all relevant interactive-use endpoints configured to require an automatic lock screen?	Yes	CSP-owned	We have configured automatic lock screens / timeout settings in all our endpoints(eg. laptops). The endpoint management solution can be used to wipe data off (remotely), lock the	Not Applicable as the control is owned by CSP (Chargebee)	UEM-06	Configure all relevant interactive-use endpoints to require an automatic lock screen.	Automatic Lock Screen	

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)			CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
UEM-07.1	Are changes to endpoint operating systems, patch levels, and/or applications managed through the organizational change management process?	Yes	CSP-owned	Chargebee has established a formal IT change management policy to ensure a formal process is followed for making any changes to systems or applications including patching,	Not Applicable as the control is owned by CSP (Chargebee)			UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	Operating Systems	
UEM-08.1	Is information protected from unauthorized disclosure on managed endpoints with storage encryption?	Yes	CSP-owned	The endpoints (eg. laptops) used within the Chargebee corporate network use customized and hardened system image, with full disk encryption enabled.	Not Applicable as the control is owned by CSP (Chargebee)			UEM-08	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption.	Storage Encryption	
UEM-09.1	Are anti-malware detection and prevention technology services configured on managed endpoints?	Yes	CSP-owned	All systems are equipped with Anti-Virus and Malware protection tools to safeguard against detrimental viruses and malware.	Not Applicable as the control is owned by CSP (Chargebee)			UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	Anti-Malware Detection and Prevention	
UEM-10.1	Are software firewalls configured on managed endpoints?	Yes	CSP-owned	Chargebee Endpoints (eg. laptops) are configured with anti-virus software that includes e-mail filtering, laptop firewalls and malware detection.	Not Applicable as the control is owned by CSP (Chargebee)			UEM-10	Configure managed endpoints with properly configured software firewalls.	Software Firewall	
UEM-11.1	Are managed endpoints configured with data loss prevention (DLP) technologies and rules per a risk assessment?	Yes	CSP-owned	Chargebee has implemented necessary controls to prevent data leakage through the following measures: - Access control:	Not Applicable as the control is owned by CSP (Chargebee)			UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	Data Loss Prevention	
UEM-12.1	Are remote geolocation capabilities enabled for all managed mobile endpoints?	Yes	CSP-owned	Chargebee has enabled Mobile Device Management for all mobile endpoints through an endpoint management solution. This solution can be used to	Not Applicable as the control is owned by CSP (Chargebee)			UEM-12	Enable remote geo-location capabilities for all managed mobile endpoints.	Remote Locate	
UEM-13.1	Are processes, procedures, and technical measures defined, implemented, and evaluated to enable remote company data deletion on managed endpoint devices?	Yes	CSP-owned	Please refer to CSP Implementation Description in UEM-12.1	Not Applicable as the control is owned by CSP (Chargebee)			UEM-13	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices.	Remote Wipe	
UEM-14.1	Are processes, procedures, and technical and/or contractual measures defined, implemented, and evaluated to maintain proper security of third-party endpoints with access to organizational assets?	Yes	CSP-owned	Suppliers' performance is monitored continuously and periodic reviews are conducted as and when necessary. In addition to an annual review, supplier information security assessments are conducted on a regular basis (as necessary) to ensure that they remain current. The relevant assessments are	Not Applicable as the control is owned by CSP (Chargebee)			UEM-14	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets.	Third-Party Endpoint Security Posture	

End of Standard