CAKE
Type 1 SOC 2
2018

REPORT ON CAKE'S DESCRIPTION OF ITS SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS RELEVANT TO SECURITY AND CONFIDENTIALITY

Pursuant to Reporting on Service Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205

December 1, 2018

Table of Contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS AT CAKE RELEVANT TO SECURITY AND CONFIDENTIALITY

To CAKE:

We have examined the attached description titled "Description of CAKE's CAKE SaaS Services System as of December 1, 2018" (the description) and the suitability of the design of controls to meet the criteria for the Security and Confidentiality principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), as of December 1, 2018. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of CAKE's ('CAKE' or 'the Company') controls are suitably designed, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

CAKE uses Amazon Web Services ("subservice organization") for data center hosting services and IT managed services. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organization are suitably designed. The description presents CAKE's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, and suitably designed at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization.

CAKE has provided the attached assertion titled "Management of CAKE's Assertion Regarding Its CAKE SaaS Services System as of December 1, 2018," which is based on the criteria identified in management's assertion. CAKE is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in CAKE's assertion and on the suitability of the design of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed to meet the applicable trust services criteria as of December 1, 2018.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to meet the applicable trust services criteria. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We did not perform any procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon. Because of their nature and inherent limitations, controls at a service organization may not prevent, or detect and correct, all errors or omissions to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the description criteria identified in CAKE's assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented as of December 1, 2018, and
b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively as of December 1, 2018, and user entities applied the complementary user-entity controls contemplated in the design of CAKE's controls as of December 1, 2018 and the subservice organization applied, as of December 1, 2018, the types of controls expected to be implemented at the subservice organization and incorporated in the design of the system.

This report is intended solely for the information and use of CAKE; user entities of CAKE's CAKE SaaS Services System as of December 1, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

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

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

A-LIGN ASSURANCE

December 20, 2018
Tampa, Florida

SECTION 2

MANAGEMENT OF CAKE'S ASSERTION REGARDING ITS SYSTEM AS OF DECEMBER 1, 2018

Management of CAKE's Assertion Regarding Its System as of December 1, 2018

December 20, 2018

We have prepared the attached description titled "Description of CAKE's CAKE SaaS Services System as of December 1, 2018" (the description), based on the criteria in items (a)(i)-(ii) below, which are the criteria for a description of a service organization's system in paragraphs 1.26 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the CAKE SaaS Services System, particularly system controls intended to meet the criteria for the Security and Confidentiality principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Technical Practice Aids*) (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. the description fairly presents the CAKE SaaS Services System as of December 1, 2018, based on the following description criteria:

   i. The description contains the following information:

      (1) The types of services provided.

      (2) The components of the system used to provide the services, which are the following:

      - *Infrastructure*. The physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks).
      - *Software*. The application programs and IT systems software that supports application programs (operating systems, middleware, and utilities).
      - *People*. The personnel involved in governance, operation, and use of a system (developers, operators, entity users, vendor personnel, and managers).
      - *Processes*. The automated and manual procedures.
      - *Data*. Transaction streams, files, databases, tables, and output used or processed by a system.

      (3) The boundaries or aspects of the system covered by the description.

      (4) How the system captures and addresses significant events and conditions.

      (5) The process used to prepare and deliver reports and other information to user entities or other parties.

      (6) If information is provided to, or received from other parties, how such information is provided or received; the role of the other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

      (7) For each principle being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the service organization's system.

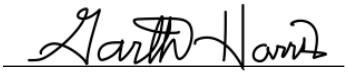
      (8) Any applicable trust services criteria that are not addressed by a control at the service organization and the reasons therefore.

      (9) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(10) Relevant details of changes to the service organization's system during the period covered by the description.

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

b. the controls stated in description were suitably designed throughout the specified period to meet the applicable trust services criteria.



Garth Harris
VP of Customer Success
CAKE

SECTION 3

DESCRIPTION OF CAKE'S SYSTEM
AS OF DECEMBER 1, 2018

OVERVIEW OF OPERATIONS

Company Background

CAKE brings clarity to digital marketing campaigns for clients around the world. Their solution empowers organizations large and small to measure the impact of their marketing efforts and make the most of their digital spend.

CAKE's culture is reflective of the people who spend their days building and supporting their products and managing their close customer relationships.

Description of Services Provided

CAKE's products and services include:

- Journey by CAKE - A cloud-based platform for collecting, analyzing and acting on digital marketing insights in real-time, providing their customers with the intelligence needed to transform anonymous consumers into known customers. Built on the trusted and proven CAKE Marketing Intelligence platform, Journey by CAKE is a cloud-based solution that collects, analyzes and empowers its customers to act on their journey data in real-time. Journey by CAKE delivers accurate and actionable insights about vital steps of the online customer journey - including the anonymous portion. With this extended view into the customer journey, customers are equipped with the intelligence to boost campaign performance and return on advertising spend
- CAKE for Networks - Marketing networks need a solution that easily captures and analyzes granular data to attribute every conversion, allowing them to pinpoint the affiliates and campaigns that are the most valuable. Customers can manage their entire affiliate network program with one tool, tracking and analyzing results, providing creative and guiding customer's digital marketing spend choices. Functionality includes: multiple payout formats; real metrics in real-time; targeted campaign control; fraud prevention; custom report calculations; role-based access and portals; and end-to-end lead generation
- Lead Distribution System - Marketers need a solution that easily captures and analyzes granular data to attribute every conversion. This allows them to pinpoint the affiliates and campaigns that are the most valuable. It empowers an organization with the intelligence needed to clarify and optimize marketing spend, properly attribute affiliate payouts, and increase online sales and lead-management efforts. Functionality includes:
    - Turn-Key System: everything needed to start and run an online lead management business
    - Incoming Lead Validation: extensive form field validation including client-side in real time
    - Fraud Detection: Stop fraudulent leads by leveraging CAKE's integrations with Forensiq, Xverify, BriteVerify and e-Hawk
    - Automated Lead Management: Single-sell, multi-sell and hybrid lead-selling options available
    - Smart Routing Technology: Maximize revenue while intelligently filling demand across all of customer's lead buyers
    - Extensive Filtering Capability: Highly customizable filtering on any field their client's collect. Perform complex logic to create compound filterable fields. Sell/route outbound leads based on geographic perimeters
    - Lead Buyer Portal: Buyers can log into a dedicated portal to manage lead returns, make deposits and access reporting

Infrastructure

Primary infrastructure used to provide CAKE's SaaS Services system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Web Servers	AWS Linux AMIs	Host files and services to support the web application
Firewalls	Cisco ASA and AWS EC2 Security Groups	Provides single authorized point of entry and filters traffic to the private networks supporting the application
Routers	Cisco CSR routers	Delivers resilient packet forwarding and encrypted cross-region connectivity for application components

Software

Primary software used to provide CAKE's SaaS Services system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Cisco AnyConnect VPN	Cisco ASA	Provides authorized point of entry and encrypted access to application private networks
SQL Server Mirroring/Backups	Windows SQL Server	Delivers near real-time replication of databases and scheduled backups to ensure data integrity
Microsoft Active Directory	Windows Server 2012 R2	Controls authentication and authorization of user activities in application infrastructure
AWS IAM and CloudTrail	Amazon Web Services	Provides identity access and authorization to application infrastructure console, logs user access and infrastructure changes

People

The CAKE staff provide support for the above service in each of the following functional areas:

Security Committee - The Security Committee is comprised of the Quarterly Information Security meeting attendees. In addition to discussing existing risks, threats and vulnerabilities, the team identifies risks mitigated by controls already in place. Remaining residual risks are summarized and reported to Senior Management in a timely manner.

Senior Management - Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision-making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior management.

CTO - The CTO is responsible for the enterprise's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.

System and Information Owners - The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. The system and information owners are responsible for reviewing, approving and when necessary, testing changes to their IT systems. Thus, they must sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware, etc.). The system and information owners must therefore understand their role in the risk management process and fully support this process.

System Users - The organization's personnel are the users of the IT systems. Use of the IT systems and data according to an organization's policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization's IT resources. To minimize risk to the IT systems, employee system and application users are provided with annual security awareness training, and customer users receive security guidance and documentation during onboarding and through support functions.

Processes

CAKE maintains a comprehensive Information Security Policy (ISP) that details the procedures that describe physical security, logical access, computer operations, change control, and data communication standards and expectations of employees. Employees are required to acknowledge their understanding and adherence to the comprehensive ISP upon hiring and re-acknowledge as significant changes are made.

Physical Security

The CAKE corporate headquarters in Newport Beach, CA and London, UK office require an authorized badge or key to gain access to the office. The offices are monitored with video surveillance. The office remains locked after business hours.

Management performs quarterly access reviews to validate that all persons with physical and logical access are active employees, and termination procedures applied ensure the timely retrieval of physical keys.

The customer-servicing production environment is housed within AWS (Amazon Web Services) who act as a sub-service organization to CAKE. AWS maintains the physical and environmental controls on which CAKE relies to protect its systems. No CAKE employees have physical access to the regional data centers currently.

To validate the continuing operating effectiveness of AWS' physical and environmental controls on which CAKE relies, Management obtains and reviews AWS' independent SOC 2 auditor's report on an annual basis for testing exceptions that would require further investigation and discussion with the service provider.

Logical Access

CAKE uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Employee access to the AWS environment is controlled, by role, via the AWS IAM (identity management) authentication tool. User, role-based, access is controlled in the application and authenticates to the database.

All assets, both production and corporate, are tracked and the inventory receives routine updating. Each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Passwords must conform to defined, complex, password standards and are enforced through parameter settings in the AWS administrator dashboard and within the application.

Remote access into the production environment is tightly restricted to only authorized workers based on their role. Workers accessing the production and development systems remotely require either VPN to access or a second-factor authentication mechanism in the form of token if not accessing via white-listed IP and VPN, along with user ID and complex password.

On a quarterly basis, managers perform access reviews for all workers with system access to assess the appropriateness of the access and permission levels and request modifications based on the principle of least-privilege, whenever necessary.

Computer Operations - Backups

CAKE replicates its application and database across multiple data centers and regions within the AWS environment. In addition, full data backups are performed nightly. Applications deployed to the AWS platform are automatically backed up as part of the managed services process on secure, access controlled, and redundant storage.

Data is spread across data center locations within AWS. Nightly backups are retained for specified intervals, and failure alerts are received by the Director of Engineering and his designees. Failed backups are investigated and resolved in a timely manner.

CAKE utilizes continuous monitoring tools with alerting enabled to assess system health and data throughput which would signal if there were backup system issues. In addition, Management reviews the testing performed by independent auditors to validate the operating effectiveness of the AWS backup and recovery.

Computer Operations - Availability

CAKE monitors the capacity utilization of physical and computing infrastructure to ensure that service delivery matches service level agreements by monitoring the AWS Dashboard, related metrics and alerts. CAKE evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers.

CAKE utilizes the vendor alerts and AWS Dashboard for System Metrics health tool to monitor the firewall, application and database servers and infrastructure routers and switches. Packets per second and CPU Load are monitored on the network along with the servers' memory usage, RAM and disk space.

Additionally, multiple monitoring tools are deployed on the application and DevOps receives and reviews all application/web server pre-defined error alerts and takes action to remediate in accordance with the incident response procedures, as needed.

CAKE has implemented an Incident Response policy and procedures to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents.

Change Control

CAKE maintains documented Infrastructure and Code Change Development policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing, code reviews, and user acceptance testing results, whenever applicable, are documented and maintained with the associated change request.

Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers. It also facilitates the code review process which is required for all changes.

Infrastructure changes are performed by CAKE's infrastructure as a service provider, AWS, who houses the CAKE production environment within AWS data center locations. AWS is responsible for applying firmware and security patches; however, CAKE actively monitors vendor and security industry vulnerability notifications impacting its infrastructure servers, routers, databases and operating systems to ensure timely patching by AWS personnel. In addition, Management will review the testing performed by independent auditors to validate the operating effectiveness of the AWS backup and recovery controls.

Data Communications

The CAKE infrastructure was architected with data encrypted communication channels between the application and database. All unnecessary communication ports and services have been disabled throughout the infrastructure stack. IP white-listing is used to only allow traffic from authorized devices and locations. Remote access is gained by a limited number of authorized administrators who must provide a second-factor authentication mechanism, in the form of token, along with user ID, complex password, as well as the recognized IP address for each system being used to access remotely. AWS config is utilized to alert administrators of all configuration changes made to production servers. Unexpected and potentially unauthorized changes are investigated in a timely manner.

CAKE utilizes AWS Cloudsploit to identify development and production environment vulnerabilities, including insecure connectivity protocol, on an ongoing basis. Management investigates and resolves medium and high-risk vulnerabilities noted in a timely manner.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. As noted above, CAKE utilizes only encrypted channels to process data within its architecture. CAKE does not allow live PII in its development data therefore encryption of data is not required at this stage.

Systems supporting the application and data respective to each customer are replicated across multiple regions within the AWS architecture as part of CAKE's focus on ensuring customer application and data resiliency.

Boundaries of the System

The scope of this report includes the CAKE SaaS services system performed in the Newport Beach, CA and London, UK facilities.

AWS hosts the CAKE infrastructure in their data centers, and CAKE utilizes several IT managed services provided by AWS (e.g. infrastructure device patching, replication and backup services, AWS CloudWatch, AWS Config, and others as outlined in this system description). The scope of this report does not include the processes and controls performed by AWS.

Significant Events and Conditions

CAKE has implemented automated and manual procedures to capture and address significant event and conditions. In addition, detailed monitoring and risk assessment procedures are in place to provide management with detailed information that impacts the SAAS system.

Please see the procedures, monitoring, and risk assessment procedures described in the relevant sections of this report for further details.

Preparation and Delivery of Reports and Data

CAKE utilizes the services and procedures described above to capture, prepare, and deliver reports and other information (described in the data section above) to user entities and other parties.

Subservice Organizations

The data center hosting services and IT managed services provided by AWS (e.g. infrastructure device patching, replication and backup services, AWS CloudWatch, AWS Config, and others as outlined in this system description) are monitored by management; however, they have not been included in the scope of this review. The following criteria and controls are expected to be implemented by AWS.

Subservice Organization Controls		
Principle	**Criteria**	**Applicable Controls**
Common Criteria/ Security	CC5.5	Physical access to data centers is approved by an authorized individual. Physical access is revoked within 24 hours of the employee or vendor record being deactivated. Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. Physical access points to server locations are managed by electronic access control devices. Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Common Criteria / Security	CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and confidentiality.

Significant Changes in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

CONTROL ENVIRONMENT

Integrity and Ethical Values

CAKE has established the following controls in order to incorporate the ethical values of the executive team throughout the organization:

- Formally, documented code of conduct communicates entity values and behavioral standards to personnel
- Comprehensive Information Security policies and procedures require employees to sign an acknowledgment form upon hiring and annually to confirm that they understand their responsibility for adhering to the policies and procedures contained within the manual
- Employees are required to sign a Confidentiality Agreement and non-disclosure statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties
- Pre-hire screening of all potential employees includes thorough background investigations is performed for employees as a component of the hiring process

Commitment to Competence

CAKE has established the following controls in order to incorporate the commitment to competence of the executive team throughout the organization:

- Management screens all technical candidates thoroughly to ensure that they possess the requisite skills to fulfill their responsibilities at CAKE
- Annual Security Awareness Training is attended by all personnel which focuses on maintaining the security and confidentiality of the proprietary and customer-servicing systems and related data
- Management supports employee training required to maintain technical proficiency and professional licenses held by employees
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of the CAKE internal and information security controls

Management's Philosophy and Operating Style

CAKE has established the following controls in order to incorporate the philosophy and operating style of the executive team throughout the organization:

- Job descriptions and annual performance reviews provide CAKE employees with a clear understanding of their job roles and responsibilities, their impact and responsibility for the security and confidentiality of systems and data, and periodic feedback on how they are meeting expectations for the same
- Business and industry risks discussed during the annual management risk assessment meetings, and issues discussed that impact all employees are communicated to the employee base via conferences or e-mail by Management
- Annual Security Awareness Training is attended by all personnel which focuses on maintaining the security and confidentiality of the proprietary and customer-servicing systems and related data
- CAKE's management team has frequent, direct communication via "stand-up" and similar meetings with employees to ensure employees understand the most critical tasks and receive clear guidance from management on those tasks

Organizational Structure and Assignment of Authority and Responsibility

CAKE has established the following controls in order to ensure that the organization structure and personnel accountability is conveyed throughout the organization:

- Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed

- Key controls that help ensure the security and confidentiality of the products and services provided to customers are assigned to employee “owners” who are responsible for the timely execution of the controls
- In addition to the annual Security Awareness Training, the employee-base would receive notification in the event that CAKE experienced a significant security breach or other incident in accordance with the Incident Response policy and procedures
- Key members of the IT team have been trained on how to respond to and evidence CAKE’s response to all security incidents

Human Resources Policies and Practices

CAKE has established the following controls in order to ensure that the Human Resources policies and procedures are adequately communicated throughout the organization:

- New employees are required to sign acknowledgement forms for the Confidentiality Agreement and Code of Conduct following new hire orientation within the first week of employment
- Employees receive periodic reviews by their supervisors inclusive of discussing any deficiencies noted in the execution of the CAKE internal and information security controls
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

RISK ASSESSMENT

CAKE holds an annual risk assessment that quantifies the impact and probability of each risk, the controls in place that mitigate each risk, and management’s plan of action with regards to all residual risks over the next twelve months. CAKE identifies and manages risks that would jeopardize the achievement of strategic objectives and risks to the Information Technology (IT) infrastructure supporting its products, as well as, specific fraud risks that could threaten the security and confidentiality of customer data. CAKE identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

Management holds quarterly Risk and Security Team meetings which include key members of the executive team as well as other key individuals to address the IT risks identified and tracked via the automated ticket workflow management system.

This process has identified risks resulting from the nature of the services provided by CAKE, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance risk - legal and regulatory changes

TRUST SERVICES PRINCIPLES AND CRITERIA

In-Scope Trust Services Principles

Common Criteria (to the Security and Confidentiality Principles)
The security principle refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.

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

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of CAKE's SAAS system; as well as the nature of the components of the system result in risks that the criteria will not be met. CAKE addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, CAKE's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Control Activities Specified by the Service Organization

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC1.0	**Common Criteria Related to Organization and Management**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and confidentiality.	A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. Reporting relationships and organizational structures are reviewed at least on an annual basis by management. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews job descriptions at least on an annual basis and makes updates, if necessary.
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and confidentiality.	A documented organizational chart is in place to assign responsibility and delegate lines of authority to personnel. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews job descriptions at least on an annual basis and makes updates, if necessary.
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security confidentiality and provides resources necessary for personnel to fulfill their responsibilities.	Job requirements are documented in the job descriptions and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process. The experience and training of candidates for employment of transfer are evaluated before they assess the responsibilities of their position. Employee evaluations are performed for employees at least on an annual basis. Employees are required to read and acknowledge information security policies upon hire and on an annual basis as a part of training compliance. Management tracks and monitors compliance with training requirements.
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and confidentiality.	An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC1.0	**Common Criteria Related to Organization and Management**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Personnel are required to sign and accept the employee handbook and code of conduct upon hire. Personnel are required to complete a background check provided by a third-party vendor upon hire.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC2.0	**Common Criteria Related to Communications**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	System descriptions are communicated to authorized external users via service level agreement (SLA) that delineate the boundaries of the system and describe relevant system components. A description of the system delineating the boundaries of the system is posted on a secure network drive and is available to personnel. A documented organizational chart is in place to communicate organizational structures, lines of reporting, and areas of authority. Reporting relationships and organizational structures are reviewed at least on an annual basis by management. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Customer responsibilities are outlined and communicated through service level agreements.
CC2.2	The entity's security and confidentiality commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Security and confidentiality commitments are communicated to external users via defined SLA. Policy and procedure are documented for significant processes are available on the entity's intranet. Employees are required to read and acknowledge information security policies and complete information security training upon hire and on an annual basis as a part of training compliance. Personnel are required to sign and accept the employee handbook and code of conduct upon hire.
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Policy and procedure are documented for significant processes are available on the entity's intranet. Roles and responsibilities are defined in written job descriptions and communicated to personnel. Management reviews job descriptions as needed and makes updates, if necessary. Personnel are required to attend annual security and confidentiality training. Customer responsibilities are outlined and communicated through service level agreements.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC2.0	**Common Criteria Related to Communications**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and confidentiality of the system, is provided to personnel to carry out their responsibilities.	Processes are monitored through service level management procedures to help ensure compliance with service level commitments and agreements. Employees are required to read and acknowledge information security policies and complete information security training upon hire and on an annual basis as a part of training compliance.
CC2.5	Internal and external users have been provided with information on how to report security and confidentiality and other complaints to appropriate personnel.	The organization's security policies and code of conduct are communicated to employees in the employee handbook. Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Defined SLAs are in place and communicated to authorized external users. The SLAs include communication procedures for reporting security and confidentiality related failure, incidents, and concerns to personnel.
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and confidentiality are communicated to those users in a timely manner.	System changes are authorized, tested, and approved by management prior to implementation. Changes are communicated to both internal and external users.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC3.0	**Common Criteria Related to Risk Management and Design and Implementation of Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC3.1	The entity (1) identifies potential threats that could impair system security and confidentiality commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks.	Documented policies and procedures are in place to guide personnel when performing the risk assessment process. A formal risk assessment is performed annually to identify threats that could impair systems security and confidentiality commitments and requirements. Identified risks are rated using a risk evaluation process and rating are reviewed by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances. Internal vulnerability scans are performed monthly and remedial actions are taken. Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested at least weekly.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC4.0	**Common Criteria Related to Monitoring Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and confidentiality and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Control self-assessments that include, but are not limited to, physical and logical access reviews, and backup restoration tests are performed on an annual basis. Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. The monitoring software is configured to alert members of the DevOps team when thresholds have been exceeded.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Logical and physical access to systems is granted to an employee as a component of the hiring process. Logical and physical access to systems is revoked as a component of the termination process. Network user access is restricted via role based security privileges defined within the access control system. Network administrative access is restricted to authorized personnel. Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity Network account lockout policies are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Network audit policy configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Network access reviews are completed by management quarterly. Application user access is restricted via role based security privileges defined within the access control system. Application administrative access is restricted to authorized personnel.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include: • Password length • Complexity Application account lockout policies are in place that include: • Account lockout duration Application access reviews are completed by management quarterly. VPN user access is restricted via role based security privileges defined within the access control system. The ability to administer VPN access is restricted to authorized personnel. Database user access is restricted via role based security privileges defined within the access control system. Database administrative access is restricted to authorized personnel. Database users are authenticated via individually-assigned user accounts and passwords. Database is configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity Database account lockout policies are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Database audit policy configurations are in place that include: • Account logon events • Account management • Logon Events Database access reviews are completed by management quarterly. Privileged access to sensitive resources is restricted to defined user roles.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and confidentiality. For those users, whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Logical and physical access to systems is granted to an employee as a component of the hiring process. Logical and physical access to systems is revoked as a component of the termination process. Control self-assessments that include, but are not limited to, logical access reviews and backup restoration tests are performed at least on an annual basis.
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Logical and physical access to systems is granted to an employee as a component of the hiring process. Control self-assessments that include, but are not limited to, logical access reviews and backup restoration tests are performed at least on an annual basis. Network user access is restricted via role based security privileges defined within the access control system. Network administrative access is restricted to authorized personnel. Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity Network account lockout policies are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Network audit policy configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events Network access reviews are completed by management quarterly. Application user access is restricted via role based security privileges defined within the access control system. Application administrative access is restricted to authorized personnel. Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include: • Password length • Complexity Application account lockout policies are in place that include: • Account lockout duration Application access reviews are completed by management quarterly. Database user access is restricted via role based security privileges defined within the access control system. Database administrative access is restricted to authorized personnel. Database users are authenticated via individually-assigned user accounts and passwords. Database is configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Database account lockout policies are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Database audit policy configurations are in place that include: • Account logon events • Account management • Logon Events VPN user access is restricted via role based security privileges defined within the access control system. The ability to administer VPN access is restricted to authorized personnel. Users can only access the system remotely through the use of the VPN, secure sockets layer (SSL), or other encrypted communication system.
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Logical and physical access to systems is granted to an employee as a component of the hiring process. Logical and physical access to systems is revoked as a component of the termination process. Control self-assessments that include physical and logical access reviews are performed at least on an annual basis.
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and confidentiality.	This criterion is managed by the subservice provider. Please refer to Section 3 for the controls managed by the subservice provider.
CC5.6	Logical access security measures have been implemented to protect against security and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	Firewall rules are implemented to control internet access and communication between the network and the public domain. External access by employee is permitted only through an authorized VPN connection.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC5.0	**Common Criteria Related to Logical and Physical Access Controls**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority.
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and confidentiality.	Industry recognized SHA encryption technology is used for defined points of connectivity and to protect communications between the production servers and users connecting to the production servers from within or external to customer networks. Administrative access to the remote access system is restricted to authorized employees.
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Internal vulnerability scans are performed monthly and remedial actions are taken. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the anti-virus software. The antivirus software is configured to scan workstations daily. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC6.0	**Common Criteria Related to System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC6.1	Vulnerabilities of system components to security and confidentiality breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Monitoring software is used to identify and evaluate ongoing system performance, security threats, changing resource utilization needs, and unusual system activity. The monitoring software is configured to alert members of DevOps team when thresholds have been exceeded. Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Data backup and restore procedures are in place to guide personnel in performing backup activities. An automated backup system is utilized to perform scheduled system backups. Full backups of certain application and database components are performed daily, and mirroring is performed continuously. IT personnel monitor the success or failure of backups and are notified of backup job status via e-mail notifications. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software is configured to scan workstations daily. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. Firewall rules are implemented to control internet access and communication between the network and the public domain.
CC6.2	Security and confidentiality incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident. A ticket tracking application is utilized to track and respond to incidents. Resolution of events is communicated to users within the corresponding ticket.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC6.0	**Common Criteria Related to System Operations**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Entity policies include probation, suspension, and termination as potential sanctions for employee misconduct.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC7.0	**Common Criteria Related to Change Management**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
CC7.1	The entity's commitments and system requirements, as they relate to security, and confidentiality are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	Documented change control policies and procedures are in place to guide personnel in the handling system changes. System changes are authorized, tested, and approved by management prior to implementation.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and confidentiality.	Management has defined a formal risk management process that specifies the process for evaluating risks based on identified threats and the specified tolerances. A formal risk assessment is performed annually to identify threats that could impair systems security and confidentiality commitments and requirements. Identified risks are rated using a risk evaluation process and rating are reviewed by management. Management develops risk mitigation strategies to address risks identified during the risk assessment process. See additional controls managed by the subservice provide in Section 3.
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and confidentiality.	Documented escalation procedures for reporting security incidents are in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and confidentiality commitments and system requirements.	Documented change control policies and procedures are in place to guide personnel in the handling system changes. System change requests are documented and tracked in a ticketing system. System changes are tested prior to implementation. Types of testing performed depend on the nature of the change. Changes are approved by management prior to implementation. Changes are communicated to both internal and external users.

COMMON CRITERIA TO ALL IN-SCOPE TRUST SERVICES PRINCIPLES		
CC7.0	**Common Criteria Related to Change Management**	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Development and test environments are physically and logically separated from the production environment. Access to implement changes in the production environment is restricted to authorized IT personnel. File integrity monitoring software is utilized to help detect unauthorized changes within the production environment. Prior code is held in the repository for rollback capability in the event that a system change does not function as designed.

C1.0	ADDITIONAL CRITERIA FOR CONFIDENTIALITY	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
C1.1	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.	The entity creates test data using data masking software that replaces confidential information with test information prior to the creation of test databases. Confidentiality policies and procedures have been documented for guiding employees in data confidentiality best practices.
C1.2	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Logical and physical access to systems is granted to an employee as a component of the hiring process. Logical and physical access to systems is revoked as a component of the termination process. Network user access is restricted via role based security privileges defined within the access control system. Network administrative access is restricted to authorized personnel. Network users are authenticated via individually-assigned user accounts and passwords. Networks are configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Complexity Network account lockout policies are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Network audit policy configurations are in place that include: • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events

C1.0	ADDITIONAL CRITERIA FOR CONFIDENTIALITY	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		Network access reviews are completed by management quarterly. Database user access is restricted via role based security privileges defined within the access control system. Database administrative access is restricted to authorized personnel. Database users are authenticated via individually-assigned user accounts and passwords. Database is configured to enforce password requirements that include: • Password history • Password age (minimum & maximum) • Password length • Password complexity Database account lockout policies are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Database audit policy configurations are in place that include: • Account logon events • Account management • Logon Events Application user access is restricted via role based security privileges defined within the access control system. Application administrative access is restricted to authorized personnel. Application users are authenticated via individually-assigned user accounts and passwords. The application is configured to enforce password requirements that include: • Password length • Complexity Application account lockout policies are in place that include: • Account lockout duration Application access reviews are completed by management quarterly. VPN user access is restricted via role based security privileges defined within the access control system.

C1.0	ADDITIONAL CRITERIA FOR CONFIDENTIALITY	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
		The ability to administer VPN access is restricted to authorized personnel. Privileged access to sensitive resources is restricted to defined user roles. Awareness training is provided to personnel around the policy and usage of personal information.
C1.3	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.	Application security restricts output to approved roles or user IDs. Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority. Transmission of digital output beyond the boundary of the system occurs through the use authorized software. Use of removable media is prohibited by policy except when authorized by management.
C1.4	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.	Security and confidentiality commitments regarding the system are included in related party and vendor specific service level agreements.
C1.5	Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.	Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available.
C1.6	Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	The Chief Information Security Officer is responsible for changes to confidentiality practices and commitments. A formal process is used to communicate confidentiality changes to users, related parties, and vendors. Related party and vendor systems are subject to review as part of the vendor risk management process. Attestation reports (SOC 2 reports) are obtained and evaluated when available.
C1.7	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.	The entity establishes written policies related to retention periods for the confidential information it maintains.

C1.0	ADDITIONAL CRITERIA FOR CONFIDENTIALITY	
Control Point	**Criteria**	**Control Activity Specified by the Service Organization**
C1.8	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.	Confidential information is maintained in locations restricted to those authorized to access. The entity establishes written policies related to the disposal of the confidential information it maintains. The entity purges confidential data stored on backup tapes and backup drives, per a defined schedule.

MONITORING

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

On-Going Monitoring

As noted throughout the system description, CAKE has deployed a number of system and data monitoring tools that control owners are responsible for monitoring and responding in a timely fashion. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications. Issues noted that require changes to be made to information systems supporting customers or the CAKE infrastructure are tracked via the ticketing system and adhere to the change management procedures and controls through resolution.

Management's close involvement in CAKE's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure the security and confidentiality of the systems and data and to maximize the performance of CAKE's personnel. The monthly Risk and Security Team meetings are a key component of CAKE's monitoring of the monitoring tools, the risk and threat landscape, and the execution of controls by CAKE personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

INFORMATION AND COMMUNICATION SYSTEMS

CAKE's management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities pertaining to internal controls. This includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to a higher level within CAKE. Key controls that help ensure the security and confidentiality of the products and services provided to customers are assigned to employee "owners" who are responsible for the timely execution of the controls.

Management believes that open communication channels help ensure that exceptions are reported and acted on in a timely fashion. To reinforce the importance of timely communication, formal communication tools such as organizational charts, employee handbooks, training classes and annual performance reviews are in place. Management's communication activities are made electronically, verbally, and through the actions of management.

CAKE provides guidance to customers during the onboarding process to educate them on how to securely use CAKE applications and obtain data in a secure manner. CAKE has also established procedures for the communication to clients in the event that systems or services will be unavailable for a period of time. Examples would include e-mails to impacted customers in the event of a disaster or during a scheduled system maintenance window.

COMPLEMENTARY USER ENTITY CONTROLS

CAKE's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Principles related to CAKE's services to be solely achieved by CAKE control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of CAKE.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Principles described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to CAKE.
2. User entities are responsible for notifying CAKE of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of CAKE services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize CAKE services.
6. User entities are responsible for providing CAKE with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying CAKE of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of CAKE was limited to the Trust Services Principles and related criteria and control activities specified by the management of CAKE and did not encompass all aspects of CAKE's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities were performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Determine whether the criteria are relevant to the user entity's assertions; and
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria.