A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
Appspace Holdings, Inc.

Date:
2025

APPSPACE

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

August 1, 2024 to July 31, 2025

Table of Contents

SECTION 1

ASSERTION OF APPSPACE HOLDINGS, INC. MANAGEMENT

ASSERTION OF APPSPACE HOLDINGS, INC. MANAGEMENT

August 5, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within Appspace Holdings, Inc.'s ('Appspace' or 'the Company') Appspace Workplace Experience Platform throughout the period August 1, 2024 to July 31, 2025, to provide reasonable assurance that Appspace's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*, and Appspace's compliance with the commitments in its Privacy Notice. Our description of the boundaries of the system is presented below in "Appspace Holdings, Inc.'s Description of Its Appspace Workplace Experience Platform throughout the period August 1, 2024 to July 31, 2025" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period August 1, 2024 to July 31, 2025, to provide reasonable assurance that Appspace's service commitments and system requirements were achieved based on the trust services criteria. Appspace's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "Appspace Holdings, Inc.'s Description of Its Appspace Workplace Experience Platform throughout the period August 1, 2024 to July 31, 2025".

Appspace uses Google Cloud Platform ('GCP') and Microsoft Azure ('Azure') to provide cloud hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Appspace, to achieve Appspace's service commitments and system requirements based on the applicable trust services criteria and Appspace's compliance with the commitments in its Privacy Notice. The description presents Appspace's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Appspace's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Appspace's service commitments and system requirements based on the applicable trust services criteria and Appspace's compliance with the commitments in its Privacy Notice. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Appspace's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period August 1, 2024 to July 31, 2025 to provide reasonable assurance that Appspace's service commitments and system requirements were achieved based on the applicable trust services criteria and Appspace's compliance with the commitments in its Privacy Notice, if complementary subservice organization controls and complementary user entity controls assumed in the design of Appspace's controls operated effectively throughout that period.

Sam Baxter

_____

Sam Baxter
Chief Information Security Officer
Appspace Holdings, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Appspace Holdings, Inc.:

Subject

We have examined Appspace Holdings, Inc.'s ('Appspace' or 'the Company') accompanying assertion titled "Assertion of Appspace Holdings, Inc. Management" (assertion) that the controls within Appspace's Appspace Workplace Experience Platform were effective throughout the period August 1, 2024 to July 31, 2025, to provide reasonable assurance that Appspace's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*, and Appspace's compliance with the commitments in its Privacy Notice.

Appspace uses GCP and Azure to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Appspace, to achieve Appspace's service commitments and system requirements based on the applicable trust services criteria and Appspace's compliance with the commitments in its Privacy Notice. The description presents Appspace's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Appspace's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Appspace, to achieve Appspace's service commitments and system requirements based on the applicable trust services criteria and Appspace's compliance with the commitments in its Privacy Notice. The description presents Appspace's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Appspace's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Appspace is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Appspace's service commitments and system requirements were achieved. Appspace has also provided the accompanying assertion (Appspace assertion) about the effectiveness of controls within the system. When preparing its assertion, Appspace is responsible for selecting, and identifying in its assertion, the applicable trust services criteria, for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system, and complying with the commitments in its Privacy Notice.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and its compliance with the commitments in its Privacy Notice. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Appspace's Workplace Experience Platform were suitably designed and operating effectively throughout the period August 1, 2024 to July 31, 2025, to provide reasonable assurance that Appspace's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Appspace's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Appspace's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Appspace, user entities of Appspace's Workplace Experience Platform during some or all of the period August 1, 2024 to July 31, 2025, business partners of Appspace subject to risks arising from interactions with the Workplace Experience Platform, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

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

A-LIGN ASSURANCE

Tampa, Florida
August 5, 2025

SECTION 3

APPSPACE HOLDINGS, INC.'S DESCRIPTION OF ITS WORKPLACE EXPERIENCE PLATFORM THROUGHOUT THE PERIOD AUGUST 1, 2024 TO JULY 31, 2025

OVERVIEW OF OPERATIONS

Company Background

Appspace was founded in 2002, headquartered in Tampa, Florida, with offices in the United States, United Kingdom, United Arab Emirates (UAE), Spain, Portugal, and Malaysia, plus remote employees in other countries. Appspace helps nearly 3,000 customers and many of the Fortune 500 deliver a modern workplace experience, unify brand culture, and enhance communications across teams big and small.

The Appspace Software-as-a-Service (SaaS) Workplace Experience Platform puts the focus on the employee and unifies the physical and digital workplace with intranets, digital signage and kiosks, workplace reservation, visitor management, an employee application and more on one unified platform that aims to be easy to deploy and a joy to use.

Description of Services Provided

The Appspace platform serves as a digital Workplace Experience Platform for Appspace's customers. Customers securely author and manage communications and content within the platform, which is then distributed to devices and displays and made available via the content portal.

Appspace's design allows for this to occur without any access to the customer's internal environment. Devices and endpoints reach out to the Appspace Cloud to pull down content, eliminating the need for opening ports on the customer's firewall. This modern platform provides Appspace's customers with a number of different communication channels and tools to help them manage their communications and content. A summary of Appspace's services include:

- Appspace Cloud
- Workplace Displays
- Workplace Experience
- Enterprise Messaging
- Employee Communications
- Appspace Intranet
- Application Integrations
- Security and Deployment
- Support
- Appspace Intelligence

Principal Service Commitments and System Requirements

The Appspace platform is grounded within Appspace's own security by design principles and procedures. The objective of this service is to provide Appspace customers with a quality, seamless content-delivery solution backed by proactive security principles. Appspace adopts the key trust service principles to ensure internal compliance controls are met, as well as privacy and regulatory requirements. Appspace's security commitment to their partners is reflected in their security by design principles in terms of protection mechanisms, safeguards and policies to handle the security threat landscape.

Due to the nature of these controls and how services are delivered to their customers, Appspace can maintain high response times and stay committed to customer Service Level Agreements (SLAs) to ensure minimum disruption to the customers service offering.

Appspace's security controls are reflected in the manner in which they deliver Role-Based Access Controls (RBACs) and least privileged access to the platform. The customer is easily able to manage user permissions, create analytics, and control content management. The platform is backed by a zero-trust architecture further protecting user information. A few of Appspace's controls are summarized below:

- Least privilege principle adopted to allow customers to configure access to their content
- Encrypting data at rest

- Encrypting data in flight
- Tokenization and cryptography controls
- Integrations via OAuth 2.0
- SAML 2.0 for Single Sign On (SSO)
- Secure solutions for session management, logging, auditing and incident response practices
- A myriad of internal controls to manage confidentiality, integrity and availability
- A robust set of information security policies and procedures, documents and controls

Components of the System

Infrastructure

Primary infrastructure used to provide Appspace's Workplace Experience Platform includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Google Cloud Virtual Private Cloud (VPC)	Network	Network subnets and segmentation
Google Cloud Firewalls	Network	Monitor ingress and egress traffic
Google Cloud Switches	Network	Google provisioned as part of the Cloud platform
Google Cloud Routers	Network	Google provisioned as part of the Cloud platform
Google Cloud Databases	Database	Stores production data
Google Cloud Compute Engine	Virtual Machine (VM) Instances	Deploy containers to launch the application
Google Cloud Storage	Backups	Disks storage
Google Cloud Key Management Services (KMS)	Encryption Keys	Encryption key management service

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Azure Virtual Network (VNet)	Network	Network subnets and segmentation
Azure Firewalls	Network	Monitor ingress and egress traffic
Azure Switches	Network	Azure provisioned as part of the Cloud platform
Azure Routers	Network	Azure provisioned as part of the Cloud platform
Azure Databases	Database	Stores production data
Azure Resource Groups	Virtual Machine (VM) Instances	Deploy containers to launch the application
Azure Storage	Backups	Disks storage

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Azure Key Management Services (KMS)	Encryption Keys	Encryption key management service

Software

Primary software used to provide Appspace's Workplace Experience Platform includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Google Cloud Platform	Linux	Performance, utilization, and capacity monitoring for the Appspace production environment
Azure	Windows	Performance, utilization, and capacity monitoring for the Appspace production environment
Antivirus	Third-party Software	Antivirus solution for Appspace endpoints
Security Monitoring	Third-party Software	Intrusion detection protecting the Appspace production environment
Ticketing System	Third-party Software	Change management tracking and ticketing software
Human Resources	Third-party Software	Human Resource (HR) Software
System Monitoring	Third-party Software	Security Information and Event Management (SIEM) solution to centralize logs and alerts
Vulnerability Scanning	Third-party Software	Internal and external vulnerability scanning solution
Source Code Repository	Third-party Software	Continuous integration/Continuous Deployment CI/CD source code repository for software development
Mobile Device Management	Third-party Software	Policies pushed to mobile devices
Identity Management	Third-party Software	Identity management solution for centralized user provisioning and authentication

People

Appspace has a staff of approximately 400 employees throughout the world, though predominantly in the United States. Appspace's philosophy is grounded in service quality designed to deliver a scalable, robust and seamless content driven solution to their customers. This philosophy is based on the company's core values which are identified below:

- Service Excellence - treat each other, customers, and partners fairly.
- Principled - act ethically and with integrity and do the right thing.
- Adaptable - remain flexible and resilient in the presence of change.
- Camaraderie - check egos and have fun inside and outside the office.
- Empowerment - trust employees and encourage leadership.

Data

The Appspace platform provides digital content templates to its Business-to-Business (B2B) customers to add their own custom content. B2B customers log in to the Appspace portal over a secure Hypertext Transfer Protocol Secure (HTTPS) web browser and have the ability to post, upload, and modify content.

Customer data is encrypted at rest using the cloud hosting service provider's provisioned Advanced Encryption Standard (AES) 256 encryption standard and Data Encryption Keys (DEKs). Appspace supports Transport Layer Security (TLS) 1.2 and TLS 1.3 for data in transit. Previous versions of TLS have been depreciated.

Client data managed within the Appspace platform is managed, processed, and stored in accordance with data protection and privacy policies in line with specific requirements established within customer contracts.

Privacy Commitments

The following table describes the information included as part of the Workplace Experience Platform of Appspace:

Client Data	
• First name, last name and e-mail address • Additional data elements are based on a per customer basis and their use of different Appspace products	• Role-based access controls which provides a list of data subjects assigned to access the platform • The Appspace Analytics Dashboard provides user activity-based reporting • The customer Portal Admin is able to review data subjects with access to the platform • A list of data subjects with valid accounts can be exported by the customer Portal Admin

The cloud hosting service provider provides a service for Appspace to securely transmit, process and store this information. This is a B2B platform where the data controller is responsible for notifying its employees of their privacy policy.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to Appspace's policies and procedures that define how services should be delivered. These are located on the Company's wiki site and Intranet and can be accessed by any Appspace team member.

Physical and Environmental Security

The in-scope system and supporting infrastructure is hosted by GCP and Azure. As such, GCP and Azure is responsible for the physical and environmental security controls for the in-scope system. Refer to the "Subservice Organizations" section below for further information.

Logical Access

The implementation of logical security controls is managed within two distinct areas: internal controls and external controls.

Internal Controls

Logical controls directives are based on Appspace's data classification and access control policies. These technical controls are designed to ensure the production environment is securely segmented from other internal systems. These technical controls are based on a zero-trust architecture, further ensuring privilege access to systems requires a number of additional identification, authentication, and authorization steps prior to being granted access to the system.

External Controls

Appspace's platform has been designed with security at the forefront of its service offering. With that in mind, Appspace is able to offer their customers the ability to configure a role-based access model when it comes to managing and publishing content. These granular controls allow the customer the ability to securely manage access to the platform.

Process and Policy Controls

Appspace leverages least privilege and role-based access principles when managing access to its system and services. User access and privileged access is reviewed quarterly. Administrators need to be granted privileges approved by the security team and are required to authenticate against Google's login process and Multi-Factor Authentication (MFA) using a physical token. Alerting and monitoring of privileged access users are captured and stored. Administrators are required to authenticate using a physical token when authenticating to production systems. SSO is utilized internally to manage authentication and password policies for Appspace users.

Human Resources Controls

Appspace's HR process is outlined in its global code of conduct and employee handbook. The handbook is for internal distribution only and covers a myriad of controls which employees are required to review and sign upon hire and on an annual basis. These controls include a code of conduct, disciplinary and sanction policies, as well as controls when handling confidential or private data as outlined in the information security and acceptable use policies.

Computer Operations - Backups

Appspace's cloud hosting service provider offers the opportunity to host the platform within geographically redundant data centers. This architecture enables Appspace to recover their backups in an alternate processing zone in the event the cloud provider's primary processing zone experienced an outage. The Appspace platform takes snapshots every four hours and retains these backups for 30 days. Backup snapshots are stored in an encrypted format and are automatically tested for restoration. Manual restoration testing of backup snapshots is completed as a component of disaster recovery plan testing that occurs annually.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information security incidents. Procedures exist to identify, report, and act upon data security breaches and other security incidents. Incident response procedures are in place to identify and respond to incidents on the network. Testing of the incident response plan occurs on an annual basis to ensure effectiveness.

Appspace monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery meets SLAs. Appspace utilized autoscaling to ensure availability of systems and processing. In addition, Appspace evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Disk storage

- Infrastructure capacity
- Network bandwidth
- CPU utilization

Change Control

Appspace maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include a change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, approval procedures, and segregation of duties requirements during deployment.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality Assurance (QA) testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request ticket. Development and testing are performed in an environment that is logically separated from the production environment. Test data is used in development and testing environments to replicate production data. Production data is never used for testing purposes. Management approves changes prior to migration to the production environment and documents those approvals within the change request ticket.

Version control software is utilized to maintain prior versions of source code 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 made by developers. Role-based access controls are in place to restrict access within the source code software.

Data communications

Firewall rule sets are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network Address Translation (NAT) functionality is utilized to manage internal and external Internet Protocol (IP) addresses. Administrative access to the firewall is restricted to authorized employees. Firewall rule sets are reviewed on a bi-annual basis by the security and cloud operations teams. Network subnetting is configured for additional network segmentation within the production network.

Redundancy is built into the system infrastructure supporting the data center services to help ensure there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted on an annual basis by a third-party to measure the security posture of the target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology. The third-party vendor’s approach begins with a vulnerability analysis of the target system to determine what application and network vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside and inside the network.

Application and operating system vulnerability scanning is performed using a third-party tool on a live basis and patched on a quarterly basis in accordance with Appspace policies. The third-party tool uses industry standard scanning technologies. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and On-Demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Appspace system are implemented through the change management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Vulnerabilities identified during penetration testing and vulnerability scanning are reviewed by the security team. Vulnerabilities are scored according to Common Vulnerability Scoring System (CVSS) scoring timeline to determine the impact and severity of the vulnerability. Testing is completed prior to updates released into production and in accordance with Appspace's patch management policy.

Boundaries of the System

The scope of this report includes the Appspace Workplace Experience Platform performed at the Tampa, Florida and Kuala Lumpur, Malaysia facilities.

This report does not include the cloud hosting services provided by GCP at the Iowa, United States; London, United Kingdom; St. Ghislain, Belgium; Dammam, Saudi Arabia; Sydney, Australia; Singapore; Oregon, United States; Quebec, Canada; and South Carolina, United States facilities.

This report does not include the cloud hosting services provided by Azure at the Iowa, United States; Paris, France; and New South Wales, Australia facilities.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Appspace's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Appspace's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policies and procedures, codes of conduct, and by example.

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

- Formally documented policies and procedures and code of conduct communicate entity values and behavioral standards to personnel. Disciplinary and sanction policies are defined for employee misconduct.
- Policies and procedures require employees to sign an acknowledgment form upon hire and on an annual basis thereafter indicating they have been given access to the global code of conduct and employee handbook and understand their responsibility for adhering to the policies and procedures contained within the handbook.
- Employees are required to sign a non-disclosure agreement upon hire.
- Background checks are performed for employees as a component of the hiring process in accordance with the laws and regulations in which the employee resides.
- Employees are required to successfully complete a security awareness training program upon hire and on an annual basis thereafter. Training material includes industry standard security principles.

Commitment to Competence

Appspace's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the required skills and knowledge.

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

- Management has considered the competence levels for job roles and translated the required skills and knowledge levels into written job descriptions.
- Additional OWASP security training is required upon hire and annually thereafter to develop the skill level of Developers and QA personnel.
- Employees have access to additional training resources to further develop their skill sets and professional development.

Management's Philosophy and Operating Style

Appspace's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks and management's attitudes toward information processing, accounting functions, and personnel.

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

- Management is briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole.
- Key Executive Management stakeholders are included within the ISMS Steering Committee to remain current on security initiatives.

Organizational Structure and Assignment of Authority and Responsibility

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

Appspace's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

- Organizational charts are in place to communicate areas of authority and responsibility.
- Organizational charts are communicated to employees on the Company's HR system and Intranet site and are updated as additional personnel are hired, terminated, and/or transferred internally.

Human Resources Policies and Practices

Appspace's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensure the service organization operates at maximum efficiency. Appspace's HR policies and practices include employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgement forms for the global code of conduct and employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Performance evaluations for each employee are performed on an annual basis.

- Employee onboarding procedures are in place to define the access request and approval process and are documented in an access request ticket.
- Employee termination procedures are in place to guide the termination process and are documented in a termination ticket.
- Access reviews are completed upon an internal departmental transfer to ensure access rights remain authorized.

Risk Assessment Process

Appspace's risk assessment process identifies and manages risks that could potentially affect Appspace's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Appspace identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

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

- Inherent and Residual Risk - a risk management process reviews inherent risks and defines residual risks
- Operational Risk - changes in the environment, staff, or management personnel
- Strategic Risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes

The security team is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Appspace actively identifies and mitigates significant risks through the implementation of various initiatives and continuous communication with leadership and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Appspace's Workplace Experience Platform; as well as the nature of the components of the system result in risks that the criteria will not be met. Appspace addresses these risks through the implementation of suitably designed internal 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, Appspace's management identifies the specific inherent risks of the organization and applies the controls necessary to address the residual risks.

Information and Communications Systems

Information and communication is an integral component of Appspace's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Appspace, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Executive management meets to monitor and report on key objectives of the organization. The security team meets weekly to identify new policies, procedures, controls, and strategic initiatives to remain current on emerging threats and vulnerabilities. Town Hall, All Hands, and Product Update meetings occur regularly to communicate companywide updates to employees. Additional company information is available for employees on the internal Intranet for employees to access.

Specific information systems used to support Appspace's Workplace Experience Platform are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Appspace's 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

Appspace's management conducts quality assurance monitoring on a regular basis and additional controls are implemented based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through team meetings, internal conference calls, and informal notifications.

Management's close involvement in Appspace's operations helps to identify significant variances from expectations regarding internal controls. Management evaluates the facts and circumstances related to any suspected control breakdown. A decision to address 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 legal compliance and to maximize the performance of Appspace's personnel.

Reporting Deficiencies

An internal tracking system 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 system.

Changes to the System Since the Last Review

No changes have occurred to the system and services provided to user entities since the organization's last review.

Incidents Since the Last Review

No incidents have occurred to the system and services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common/Security, Availability, Confidentiality, and Privacy criteria were applicable to Appspace's Workplace Experience Platform.

Subservice Organizations

This report does not include the cloud hosting services provided by GCP at the Iowa, United States; London, United Kingdom; and St. Ghislain, Belgium; Dammam, Saudi Arabia; Sydney, Australia; Singapore; Oregon, United States; Quebec, Canada; and South Carolina, United States facilities.

This report does not include the cloud hosting services provided by Azure at the Iowa, United States; Paris, France; and New South Wales, Australia facilities.

Subservice Description of Services

GCP or Azure provide cloud hosting services, which include implementing physical security controls for the housed in-scope systems. Controls include but are not limited to requiring visitor sign ins, requiring badges for authorized personnel, and monitoring and logging of physical access to the facilities.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by GCP to provide reasonable assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	The organization has policies and guidelines that govern how to keep the organization's physical workplaces, facilities, and property safe.
		Data center server floors, network rooms and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, secondary identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
		Data centers are continuously staffed and monitored by security personnel through the use of real time video surveillance and/or alerts generated by security systems.
Availability	A1.2	Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.
		Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
		Data centers are equipped with fire detection alarms and protection equipment.
		The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.
		The organization conducts disaster resiliency testing which covers reliability, survivability, and recovery on an ongoing basis (and at least annually).
		The organization has implemented business continuity measures to maintain the availability of its production infrastructure and services.

The following subservice organization controls should be implemented by Azure to provide reasonable assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors have been established.
		Security verification and check-in for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The datacenter facility is monitored 24x7 by security personnel.
Availability	A1.2	Azure has developed a Business Continuity and Disaster Recovery (BC / DR) Standard Operating Procedure and documentation that includes the defined information security and availability requirements.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		The BCP team conducts testing of the business continuity and disaster recovery plans established for Azure services, per the defined testing schedule for different loss scenario. Each loss scenario is tested at least annually. Issues identified during testing are resolved and plans are updated accordingly.
		Procedures for the continuity of critical services provided by third-parties have been established. Contracts with third-parties are periodically monitored and reviewed for inconsistencies or non-conformance. Procedures to transition between critical third-parties based on results of monitoring are established.
		A Datacenter Business Continuity Management Program defines business continuity planning and testing requirements for functions within the datacenters. Datacenters exercise, test and maintain the Datacenter Business Continuity Plan for the continued operations of critical processes and required resources in the event of a disruption at least annually. The 'Business Continuity Management Exercise and Test Program Framework' document establishes the basis and process for exercising and testing of the plans for continuity and resumption of critical datacenter processes.
		Datacenter Management teams conduct and document a resiliency assessment, specific to the datacenter's operations, on an annual basis or prior to proposed significant changes.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Datacenter Management team maintains and tests datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

Appspace management, along with the subservice organization, defines the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as SLAs. In addition, Appspace performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing third-party attestation reports over services provided by vendors and subservice organizations on an annual basis
- Monitoring external communications, such as customer complaints, relevant to the services provided by the subservice organization
- Reviewing compliance standards and contractual obligations provided by vendors and subservice organizations on an annual basis
- Annual third-party risk assessments are completed to ensure security controls provided by vendors and subservice organizations are operating effectively.

COMPLEMENTARY USER ENTITY CONTROLS

Appspace'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 Criteria related to Appspace's services to be solely achieved by Appspace control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Appspace.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria 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 Appspace.
2. User entities are responsible for notifying Appspace of changes made to technical or administrative contact information.
3. User entities are responsible for implementing SSO technologies through their Identity Provider.
4. User entities are responsible for implementing their own MFA controls, if applicable.
5. User entities are responsible for maintaining their own systems of record.
6. User entities are responsible for ensuring the supervision, management, and control of the use of Appspace services by their personnel.
7. User entities are responsible for providing Appspace with a list of approvers for security and system configuration changes for data transmission.
8. User entities are responsible for immediately notifying Appspace of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
9. User entities are responsible for content management and content displayed via the Appspace platform.
10. User entities are responsible for assigning the appropriate role-based access control settings for their users.
11. User entities are responsible for ensuring the data subject information entered into the platform is accurate and is not fraudulent.
12. User entities are responsible for notifying Appspace of a data deletion request or right to be forgotten.
13. User entities are responsible for provisioning and deprovisioning end users in the Appspace platform.
14. Users entities are responsible for adhering to Appspace's Acceptable Use Policy.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security, Availability, Confidentiality, and Privacy Categories)

Security refers to the protection of:

i. information during its collection or creation, use, processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Privacy

Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

Although the confidentiality applies to various types of sensitive information, privacy applies only to personal information.

The privacy criteria are organized as follows:

iii. *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.

iv. *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.

v. *Collection.* The entity collects personal information to meet its objectives related to privacy.

vi. *Use, retention, and disposal.* The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.

vii. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.

viii. *Disclosure and notification.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.

ix. *Quality.* The entity collects and maintains accurate, up-to date, complete, and relevant personal information to meet its objectives related to privacy.

x. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.