Service Organization Controls 3

Report

For the Period from October 1st, 2022 to September 30th, 2023

Report on the WalkMe Digital Adoption Platform
Relevant to Security, Availability, Processing
integrity, Confidentiality and Privacy

HQ
525 Market St, Floor 37,
San Francisco,
CA 94105

R&D Center
Kremenetski St 3,
Tel Aviv-Yafo,
Israel

I. Report of Independent Service Auditors

Board of Directors and Management of WalkMe

We have examined management's assertion, contained within the accompanying Management's Report of Its Assertion on the Effectiveness of Its Controls Over the WalkMe's Digital Adoption Platform (the "System") Based on the Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy (the "Assertion"), that WalkMe's controls over the WalkMe's Digital Adoption Platform (the "System") were effective throughout the period October 1st, 2022 to September 30, 2023 to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, processing integrity and privacy (applicable trust services criteria) set forth in the AICPA's TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Management's Responsibilities

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

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. Our examination was conducted 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 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 controls were not effective to achieve the Company's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company's 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.
We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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, WalkMe's controls over the WalkMe Digital Adoption Platform (the "System") were effective throughout the period October 1st, 2022 to September 30, 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Fahn Kanne Control Management Ltd.

January 31, 2024
Tel Aviv, Israel

II. WalkMe's Assertion

Management Assertion on the controls over WalkMe's System based on the AICPA Trust Services Principles and Criteria for Security, Availability, Processing integrity, Confidentiality and Privacy.

We were responsible for designing, implementing, operating, and maintaining effective controls within WalkMe's ("Company") Digital Adoption Platform, ("system") throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that company's service commitments and system requirements relevant to security, availability, processing integrity, confidentiality and privacy were achieved. Our description of the boundaries of the system is presented in WalkMe's Description of the Boundaries of its Digital Adoption Platform 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 October 1, 2022 to September 30, 2023, to provide reasonable assurance that Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Service Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria). Company'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 Section III, *WalkMe's Description of the Boundaries of its Digital Adoption Platform*.

WalkMe uses the subservice organizations uses Amazon Web Services ("AWS"), Microsoft Azure ("Azure") and Google Cloud Platform ("GCP"). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at WalkMe, to achieve WalkMe's service commitments and system requirements based on the applicable trust services criteria.

WalkMe'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 the accompanying system description.

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 October 1, 2022 to September 30, 2023, to provide reasonable assurance that WalkMe's service commitments and system requirements were achieved based on the applicable trust services criteria.

January 31, 2024

Dan Adika
CEO

DocuSigned by:
91BE84589EF147F...

III. WalkMe's Description of the Boundaries of its Digital Adoption Platform

Scope

This report describes the control structure of WalkMe (the "Company" or "WalkMe") as it relates to WalkMe Digital Adoption Platform (the "System") throughout the period October 1, 2022 to September 30, 2023 (the "specified period") for the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (the "Applicable Trust Services Criteria") as set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).
It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

Company Overview and Background

WalkMe's low-code Digital Adoption Platform ("DAP") enables organizations to leverage data to take immediate action to simplify user experiences across enterprise applications. WalkMe is designed for executives, IT organizations, and line of business managers, enabling them to take a user-first approach to software adoption to accelerate digital transformation.

Products and Services

WalkMe's primary service is a cloud-based Digital Adoption Platform offering in-application guidance, engagement, automation and analytics. The context-intelligent platform engages with users exactly when and where they need it, guiding them to any desired action within an application. All of this is accomplished without any changes to or integration with the underlying software.

Components of the system providing the defined services

As a pure software-as-a-service (SaaS) company, WalkMe offers a secure, reliable, and scalable platform that will not affect site performance. All WalkMe servers, databases, and storage are located in a top tier and secure cloud network. In order to provide customers with the greatest flexibility, WalkMe utilizes Amazon Web Services (AWS) and Google Cloud Platform (GCP).

WalkMe Digital Adoption Platform Modules:

- **Data**: Provides visibility into the organization's tech stack and business processes.

- **Action:** Create and design data-driven experiences by leveraging automation, best practice templates, UI elements and tools suitable for any application and device**.**
- **Experience:** Where WalkMe meets the end-user, through elegant experiences that engage and drive employee and customer adoption of technology**.**

WalkMe Policies Relevant to security, availability, processing Integrity, confidentiality and privacy
WalkMe management requires formal written policies for significant functions and processes.

Security, availability, processing Integrity, confidentiality, and Privacy Policies:

There is a formal process for updating, reviewing and approving the company's security policies and procedures. The process is conducted as part of the annual review, which is performed twice a year. Responsibility and accountability for developing and maintaining the policies are assigned to the relevant personnel and approved on an annual basis by the management team.

Communication:

WalkMe shares and communicates the policies to WalkMe's employees using email and a cloud-based file sharing portal. In addition, a system description and its boundaries are documented by the management. The document is reviewed, approved on an annual basis by the management team and communicated to WalkMe employees through a cloud-based file sharing portal. Security, availability, processing Integrity, confidentiality, and Privacy-related obligations are communicated to WalkMe's employees through the confidentiality and non-disclosure agreements while client obligations are communicated within their contracts. In addition, a ticketing system is available to WalkMe employees in order to report breaches of the system security, availability, processing Integrity, confidentiality, and Privacy. Customer issues are reported directly to the Support or their CSM and documented within the cloud-based system.

Security

In order to address the risks posed by the public networks such as the Internet, WalkMe has implemented different security controls (physical, administrative and technical) on all layers, to secure its services, which is governed by the following core principles. With respect to the above, security vulnerabilities cannot be totally eliminated.

Risk Assessment

WalkMe has implemented measures and procedures in order to identify potential threats of disruption to systems operation that would impair system security, availability and confidentiality commitments, prevent and mitigate threats when commercially practicable and assess the risks associated with the identified threats. Risks and threats are evaluated by key personnel within WalkMe during an annual risk assessment meeting. Action items are documented within minutes of the meeting. Minutes of the meetings are retained

Logical Access

WalkMe has established an organization-wide information security policy designed to protect information at a level commensurate with its value. The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission.

Access Control, User and Permissions Management

WalkMe manages and delivers its services using Active Directory for the backend, and AWS / GCP for the production systems. Information security controls and procedures are implemented throughout these systems to help prevent unauthorized access to data. Access to system resources is protected through a combination of several security controls such as: firewalls, VPNs, native operating system access controls, database management system security and application controls. WalkMe employees are provided with unique, personal user accounts that enable them to access the corporate network and corporate cloud account if needed. Access to other environments is restricted based on job function. Employees are provided with the minimal access rights required to carry out their duties. Access to the production environment, where information resources not deemed to be public reside, including the domain, databases and other production-related environments, is granted upon approval by the system owner. In addition, the access to the database is restricted to authorized personnel only.

Usernames and passwords are used to authenticate personnel who need to access a system or a resource. Wherever possible, a 2FA authentication is enabled and enforced to restrict access to company resources. Strong password configuration settings, where available, are enabled on the domain, application and databases. The access to the production environment servers is performed using a multifactor authentication (MFA).

Backup Storage

The access to the backup is restricted only to authorized individuals.

Revocation Process

In order to prevent unauthorized access to data, user accounts within WalkMe's various environments are disabled upon termination of employment. Termination notifications indicating the employee's expected last day are sent to the relevant functions: Management, Finance, IT and Security. Terminated employees complete a termination clearance process on their last day at WalkMe. This process includes revocation of access permissions to the systems and premises, as well as the return of the Company property, data and equipment. The HR manager confirms with the system administrator that the terminated employees' access rights have been disabled.

Recertification of Access Permissions

WalkMe has implemented an access recertification process to help ensure that only authorized personnel have access to the systems, environments and databases. Quarterly, the CISO conducts an access rights review of user access permissions on the domain, company cloud-based file drive, application and database. Additionally, quarterly, both the SRE and the IT teams generate a report listing the members of the administrative groups within the production environment which is reviewed by the management team. Employees whose job functions have evolved and who, therefore, no longer require access to particular permissions, have their access disabled.

Deployment Application and Production Environment Logical Access Management

WalkMe also developed a tool that automates the deployment or rollback of a version to the production environment. The tool utilizes defined scenarios that describe the actions to be taken for an upload or a rollback from one version to another. The application has a user management utility used to assign permissions to pre-defined groups, users and servers. The access to the application and the production servers is restricted to authorized personnel. In addition, the access to the firewall management tool is restricted to authorized personnel.

Remote Access and Encryption

WalkMe networks are protected using commercial firewalls, which are configured and administered by the Network Security team. WalkMe employees are granted remote access to the production environment based on the need-to-know and least privileges principles, and only from a dedicated secured connection. To be granted access, the employee's direct manager and the CISO need to review the request and approve it. In addition, remote site-to-site access to the production network is accomplished through a secured connection and is restricted by the use of Company's personnel only. WalkMe information security policy requires employees who are granted remote access permission to secure their work environment using antivirus software and a personal firewall, and to protect their workstation from unauthorized users. The policy prohibits employees from accessing the production network from non-secured environments. Also, traffic between client browsers and the production environment is encrypted and customer passwords are encrypted within the database.

Physical Access

***Access to the Data Center*:** WalkMe hosts its data centers in Amazon and Google GCP. WalkMe manages its data center activities in a highly secured environment, with strict access controls (both logical and physical). Servers at the data center are located in a secured location with security measures implemented to protect against environmental risks or disaster.

Visitors and Contractor Access: Visitors to the WalkMe's office are accompanied while on premises to help prevent unauthorized access to data and assets.

Security Awareness and Training

In order to help ensure that WalkMe employees are aligned with the security practices and aware of their duties, WalkMe has conducted an information security awareness campaign. In addition, the security obligations of users and the entity's security commitments to users are communicated on an annual basis through the company policy and code of conduct document.

Penetration Testing

WalkMe annual security program includes testing for security vulnerabilities by an independent security assessment service provider. Penetration tests that help to ensure the overall security status of the production environment and consistency with the confidentiality policy are performed on an annual basis. The penetration testing includes, among other things, processes to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own.

Antivirus

Where technically applicable, WalkMe uses a real-time antivirus solution Next generation EDR (Endpoint Detection and Response) and antivirus solutions to protect its personnel workstations against viruses, worms, Trojan horses and other forms of malicious code that may cause damage.

Security in the Development Life Cycle

In order to help ensure the delivery of a highly secure platform, security is an inherent part of the WalkMe software development life-cycle (SDLC). Developers are security resources with experience with secure coding and possible pitfalls.

Human Resources Hiring Practices

WalkMe human capital is the most valuable asset for the Company. The collective sum of the individual differences, life experiences, knowledge, inventiveness, innovation, self-expression, unique capabilities, and talent that WalkMe Team Members invest in their work represents a significant part of not only WalkMe culture and reputation, but of WalkMe productivity and achievement within the marketplace. Because of this, WalkMe created the LeadRight Rule. This is part of WalkMe ongoing commitment to diversity, equity, and inclusion in WalkMe hiring practices. For all director level and above positions, recruiters and hiring managers must consider multiple candidates that meet the Standards of Diversity aligned with local labor laws.

WalkMe has designed formal global hiring practices to help ensure that new, rehired or transferred employees are qualified for their functional responsibility. Where local labor law or statutory regulations permit, WalkMe may conduct criminal, credit, and/or security checks on all potential employees as well as verification of the individual's education, previous employment, and referrals. The specifics or extent of background checks performed depend on the position for which the individual is applying.

Upon acceptance of employment, all employees are required to execute a confidentiality agreement as well as acknowledge receipt and compliance with WalkMe's acceptable use policy. The confidentiality and privacy of customer data is emphasized in the policy and also during new employee orientation training. It is the responsibility of every employee or contractor to timely communicate significant issues and exceptions to an appropriate higher level of authority within the Company. Every employee has a written job description, and every job description lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by WalkMe.

Third-party Risk Management

WalkMe utilizes sub-processor entities to support WalkMe services, and has established expectations for sub-processor entities related primarily to security. The meeting of these expectations is subject to periodic review by WalkMe.

WalkMe maintains a Sub-processor Assurance Program that is tasked with reviewing the vendor security posture using ISO 27001 as the baseline. WalkMe evaluates conformance to these expectations through inspection of third-party ISO certifications and SOC 2 reports. In the case that WalkMe identifies any deviations in the performance of sub-processor controls, findings are evaluated by WalkMe and discussed with the vendor upon completion of the audit. When applicable, remediation plans are put in place to timely resolve issues. WalkMe uses appropriate contractual safeguards to ensure security and privacy obligations are met to satisfy WalkMe's obligations regarding customer data, prior to WalkMe granting such access.

Privacy Procedures

WalkMe maintains a documented privacy policy that has been approved by management, communicated to appropriate constituents and stakeholders, has been established, and is re-approved annually by management.

As a global company, WalkMe is committed to protecting the personal data of WalkMe prospects, customers, business partners and employees. In doing so, WalkMe is continually looking at ways to ensure compliance with a broad range of international data protection laws regarding the processing of personal data. The applicability of any of the foregoing data protection laws is determined on the basis of the jurisdiction in which customers operate and/or where the end users of the WalkMe Services are located and/or where the WalkMe Service is being provided from.

All applicable data protection laws have in common their ability to enhance individuals' data privacy rights by ensuring greater accountability and transparency regarding why, how and where personal data processing is taking place. As such, WalkMe is dedicated to comply with all applicable data protection laws through its privacy compliance program.

To the extent the GDPR/UK GDPR applies, WalkMe is considered the "processor" of customer data, as the customer is the entity determining the means and purposes of the processing when using WalkMe Services. Before any personal data processing which is subject to the GDPR/UK GDPR will take place, WalkMe and its customers will enter into a Data Processing Agreement ("DPA") which sets forth the

specific details of the types of personal data to be processed. WalkMe also processes certain data (as described in its privacy policy noted below) for its own purposes as a "controller".

WalkMe is devoted to continuously monitoring and updating its services, products, and the accompanying terms, policies, contracts, and documentation in order to enable compliance with the applicable data protection laws. WalkMe's privacy policy informs website users, customers, customer end users and any other relevant individual regarding the personal data collected through their engagement with WalkMe and sets forth how they can enforce their available rights under the applicable data protection laws.

Notice

WalkMe is committed to protecting the privacy of the users of WalkMe services. WalkMe privacy policy, which is publicly available on WalkMe website, explains the types of information WalkMe may collect from customers or that customers may provide when they use WalkMe Services and WalkMe practices for collecting, using, maintaining, protecting, and disclosing that information, as well as customer rights in determining what WalkMe does with the information that WalkMe collects and holds about customers.

WalkMe aims to process only adequate, accurate and relevant data limited to the needs and purposes for which it is gathered. It also aims to store data for the time period necessary to fulfill the purpose for which the data is gathered. WalkMe only collects data in connection with a specific legitimate purpose and only processes data in accordance with the Privacy Policy.

Where applicable, view and amend fair processing notices are displayed at the point when personal information is collected directly from a data subject. Since WalkMe is the data processor, the data collection and WalkMe operation is only used for providing the service for the data controller, who is responsible. WalkMe enables the customer the ability to segment the users according to specific rule set such as geographical location and provide the relevant notice to the end-user using the platform.

WalkMe notify customers via a formal channel, such as the company's website, and/or email notification letter and/or a notice in WalkMe platform for any material change in the data privacy policy. WalkMe will endeavor to provide notice of material changes to the Privacy Policy through WalkMe Site, Services and/or via an e-mail.

Choice and Consent

WalkMe is a data processor in the provision of WalkMe's services to its customers. There is no direct engagement with the customer end-users.

WalkMe only processes data of End Users on behalf of the customer (the controller). Customers are responsible for managing disclosure and notice requirements for data processed by WalkMe on behalf of the customer, when applicable, because WalkMe is not responsible for providing notice, obtaining consent, or having knowledge of what individuals have been provided notice or consented to.

Collection

In order to provide the Services to our Customers, WalkMe collects and processes certain information (which may include personal information) about WalkMe Customer's Authorized Representatives and End Users. To the extent the GDPR applies to such processing activities, WalkMe is the Processor of such data. The information collected depends on the Service used and type of user (customer or end-user).

Where the customer is an Authorized Representative accessing and using WalkMe Services, WalkMe collects name, email address and WalkMe log-in credentials and IP address.

Where the customers' end-users engage with WalkMe services, WalkMe collects your IP address, web application data (page title/URL) and geolocation (only country and city). WalkMe retains IP addresses in logs for security purposes. Additionally, the customer can also utilize special features which require collecting and storing additional personal data; ultimately, the customer can control the level of data collection.

Use, Retention, and Disposal

Data is retained in compliance with the contract between WalkMe and the customer. WalkMe will retain personal information for as long as required to provide WalkMe services and as necessary to comply with our legal obligations, resolve disputes and enforce our terms and conditions, other applicable terms of service and our policies.

WalkMe as a processor is responsible to promptly, and in any event within 90 days of termination of the contract or upon customers request, delete or return all copies of customer data, except where such copies are required to be retained in accordance with the Applicable Data Protection Legislation and provided that Processor shall ensure the confidentiality of all such Controller Data.

WalkMe notified customers when it receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, erasure, data portability, or to object to processing, each a "Data Subject Request". WalkMe will provide commercial assistance to customers by taking appropriate technical and organizational measures for the fulfillment of customers obligation to respond to requests for exercising the Data Subjects' rights as laid down by Applicable Data Protection Legislation.

Access

Access is managed centrally, and user management is done by the customer. WalkMe provides customers with an interface to create users with access to specific parts of the system, according to customer needs. The interface also provides the ability to add / remove users and manage access level permissions. A formal user access provisioning process is implemented with access level roles, which contains the permissions of the role to assign or revoke access rights for all user types to all systems and services. Provisioning individuals with access to customer personal information is the responsibility of the customer.

WalkMe takes steps to protect, enforce and maintain the security of our Services, Site, Customer information as well as the personal information of Authorized Representatives and End Users.

WalkMe uses a combination of processes, technology and physical security controls to help protect personal information from unauthorized access, use, or disclosure. Although WalkMe does our best to protect your personal information, WalkMe cannot guarantee the security of your information transmitted over the internet and any transmission is at your own risk.

WalkMe implements appropriate technical and organizational measures to protect and safeguard the customer data that is processed, against Personal Data Breaches.

WalkMe maintains its security and privacy controls and audits, pursuant to, amongst others, ISO 27001, ISO 27701, this SOC 2 type II and ISO27799 Security management in health as detailed at: https://www.walkme.com/walkme-security/or otherwise made reasonably available by WalkMe. WalkMe regularly monitors compliance with these safeguards.

Quality

Personal information collected by WalkMe is relevant, complete, and accurate for the purposes for which it is utilized to meet WalkMe's objectives. As a Data Processor WalkMe provides the Data Controller (WalkMe's Customers) with full access to their data. Through WalkMe's Insights analytics platform, the Data Controller can access and review data on all their end-users. WalkMe records the user actions on the WalkMe platform and/or user behavior on site. The data is not coming from the user itself, but rather from the way they interact with the site or an integration with the platform WalkMe is implemented on (like UUID). Hence, the right to rectify and update records data and information relating to a specific, named individual is not applicable to WalkMe. In case the platform WalkMe is implemented on will change/ update the user information - the information WalkMe records will also update. Moreover, to fully comply, WalkMe offers a deletion of end-user's data if necessary. WalkMe performs adequate due diligence on third-party sources utilized.

Monitoring and Enforcement

WalkMe is also certified under the Data Privacy Framework (EU-US, SWISS-US, UK-US), for transferring EU/SWISS/UK data to the US.

WalkMe has appointed WalkMe Germany GmBH as WalkMe's representative in the European Union for data protection matters such as inquiries, complaints, and disputes, pursuant to Article 27 of the GDPR. WalkMe maintains an up-to-date process to address inquiries, complaints, and disputes in a timely manner. WalkMe monitors the effectiveness of controls over personal information and compliance with privacy objectives. WalkMe documents and tracks inquiries, to ensure that identified issues are remediated timely.

Processing Integrity

WalkMe designed controls that prevent, or detect and correct, processing errors, to meet processing integrity commitments and system requirements, to ensure validity, accuracy, timeliness, and authorization of system processing.

Quality Assurance

WalkMe performs internal quality assurance processes associated with continuous integration to ensure meeting commitments associated with processing integrity.

Process Monitoring Systems

WalkMe utilizes file integrity monitoring (FIM) checks along with strict access controls. WalkMe Monitors the files of the customers and makes sure they have not been tampered or changed.

Authorization

Logical access to stored data is restricted to the application and database administrators. Access is managed centrally, and the provisioning is done manually within the user management systems. Segregation of duties is done between the R&D team, who develops the code, the DevOps team, who has the ability to upload code to production, and the Security team, who manage the security controls. The access rights are enforced at all levels: the network (connectivity is only allowed from a dedicated segment in the office network), the OS (specific user accounts are configured on the servers), and the application (application level authorization is enforced) levels. All of these components generate audit trails that are collected by our SIEM for analysis. The SIEM alerts on the occurrence of pre-defined scenarios, for example, failed login attempts, and logins occurring outside the office IP address or during off-hours. WalkMe output are restricted to approved authenticated users

Backup integrity

WalkMe has implemented data backup procedures using an automated system, and the incident management process is invoked upon if backups fail alert was generated. Backups are transported and stored offsite by a third-party storage provider, in case of software or data loss or system unavailability due to processing error, intentional act, or environmental event.

Processing capacity

System capacity is monitored on a daily basis using several monitoring and alerting tools — both internal (by reporting of errors to the DevOps team from the application) and using external log management, alerting platforms, cloud health monitoring and CloudTrail tools. Autoscaling is configured where applicable. Critical infrastructure components have a defined level of redundancy based on risk assessment and BCP procedures.

API Checksum

WalkMe provides an API Checksum to ensure data has not been tampered or changed. Customers can leverage these tools and verify integrity independently.

Audit Log API

WalkMe provides an audit log API, allowing the customer to import the logs into their own SIEM system and monitor it in their own environment.

Sub-Resource Integrity (SRI) security module

To protect the integrity of the static JavaScript files, WalkMe customers can enable sub-resource integrity checking (SRI) for the files retrieved from the CDN. WalkMe applies SRI by generating a signed file with the customer's certificate that contains a list of all the files and their checksum hashes that are applicable to the customer's package. When the static files are retrieved from the CDN, their checksums are verified against the checksums included in the signed file. Any files that have been modified will not load.

Software Development Lifecycle ("SDLC") and Change Management

WalkMe organizational structure enables the SDLC and application change processes to be executed by separate groups. Development is performed by the R&D teams; testing is performed by the QA teams and implementation to the Production environment is performed by the SRE and DevOps teams.

Supply Chain

WalkMe is following the ISO 20243 standard for supply chain security as part of the Open Trusted Technology Provider™ Standard (O-TTPS) Certification Program. WalkMe established a secure development lifecycle (SDLC) process, which includes security requirements and controls at every stage of the development process. This helps to ensure that WalkMe products and services are secure from the start. WalkMe also maintains compliance with ISO 20243, which is an international standard for information security management. This standard provides a framework for establishing, implementing, maintaining, and continually improving an information security management system. WalkMe regularly review and assess supply chain security measures to ensure that they are effective and up-to-date.

Support

WalkMe customer support procedures are designed to handle and resolve issues and requests timely and efficiently. These include issues that are internally identified or submitted by customers. WalkMe provides its customers with three tiers of technical support based on the customer's SLA (24 hours a day, seven days a week, 365 days a year / 12 hours a day, five days a week / during customer business hour in their primary office location).

Availability Procedures

Backup and restore

WalkMe SRE team is responsible for managing and performing backup tasks on various types of service-related data retained within the production environment to enable availability and redundancy of data. Databases are redundant within the Production environment. WalkMe application database and critical portions of the application file system are backed up daily.

On an annual basis, the SRE team performs a restoration test from an application database backup to determine that data can be recovered efficiently and in a controlled manner.

Disaster recovery

WalkMe DR approach is based on ensuring availability via usage of multiple AWS availability zones, as well as caching the content with Akamai. By doing so, WalkMe created a fully redundant setup. WalkMe annual DR Tests are scoped for production environment as well as corporate offices.

Confidentiality Procedures

WalkMe understands that confidentiality issues are significant as it relates to the services provided. Unless configured otherwise, WalkMe logs each visitor's browsing information (e.g., IP addresses, browser types, referring page). Customer data has a single classification and access is restricted to authorized personnel. Also, In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, impacted customers are notified as defined within their Service Level Agreements. A confidentiality agreement is disclaimed as it relates to contracts with datacenter service providers in accordance with WalkMe's confidentiality policy.

Monitoring

Managers at WalkMe are responsible for monitoring the quality and effectiveness of the various operations as a routine part of their activities. Performance reports and statistics are generated on a regular basis and presented to executive management for evaluation.

The Company utilizes subservice organizations to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party service organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control must be evaluated in conjunction with the Company's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Services Provided/Complementary Controls/ Monitoring Controls	Associated Criteria
- Amazon Web Services ("AWS") - Google LLC (Google Cloud Platform) - Microsoft Azure - IBM Ireland Ltd (IBM Cloud) - Akamai Technologies Inc. - Confluent, Inc. - Okta, Inc. - Datadog, Inc.	The Subservices is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, operating system, and storage devices for its cloud hosting services where WalkMe systems reside.	CC6.1- CC6.3, CC6.5- CC6.6
	The Subservices is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 - CC6.5, CC7.2
	The Subservices is responsible for ensuring data within the cloud hosting is stored in an encrypted at rest format.	CC6.6, CC6.7, C1.1
	The Subservices is responsible for ensuring access to Cloud Storage server-side encryption keys is restricted to authorized personnel.	CC6.6, CC6.7, C1.1
	The Subservices is responsible for implementing controls to restrict and protect information during transmission, movement, and removal from the underlying storage devices for its cloud hosting services where WalkMe systems reside.	CC6.7, CC7.2,
	The Subservices is responsible for monitoring any changes to the logical access controls system for the underlying network, virtualization management software, operating system, and storage devices for its cloud hosting services where WalkMe systems reside.	CC7.1

**The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.

Complementary User Entity Control (customers' responsibility)

WalkMe designed its controls with the assumption that certain controls will be the responsibility of its customers (or "user entities"). The following is a representative list of controls that are recommended to be in operation at user entities to complement the controls of WalkMe's Digital Adoption Platform. This is not a comprehensive list of all controls that should be employed by WalkMe's user entities.

Complementary User Entity Control	Associated Criteria
Logical Access: Customers are responsible for creating a username and password to access their account. Customers are responsible for adding and removing users and managing access level permissions. Customers are responsible for establishing their own usage and access policies to their WalkMe accounts. Customers are responsible for identifying approved points of contacts to coordinate with WalkMe. Customers are responsible for configuring their instance of WalkMe according to their organizations policies and procedures. Customers are responsible for performing periodic review of access and configurations for appropriateness.	CC2.1 CC5.2 CC6.1 CC6.2 CC6.3 CC6.5 CC6.6
Change Management: Customers are responsible for validating the accuracy and completeness of data contained in their WalkMe account.	CC8.1
Incident Management and security: Customers are responsible for alerting WalkMe of incidents (related to Security, Availability, and Confidentiality) when they become aware of them. Customers are responsible for monitoring or resolving the incident alerts as part of the use of the application Customers are responsible for managing content and digital assets within their WalkMe environment. Customers are responsible for configuring network and application layer firewalls within their internal environment to prevent unwanted or unauthorized traffic, such as file sharing sites. The customer is responsible for secure workflow processes surrounding data uploaded and processed within their WalkMe environment	CC4.1 CC4.2 CC6.6 CC7.2 CC7.3 CC7.4

Privacy: The customer is responsible provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The customer is responsible for the deletion of metadata in their WalkMe account. The customer is responsible for managing disclosure and noticing requirements to End Users for data stored in WalkMe services. The customer is responsible for communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. The customer is responsible for explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. The customer is responsible for obtaining explicit consent, prior to disclosure, of the data subjects for the transfer of personal information to third parties. The customer is responsible for creates and retains a complete, accurate, and timely record of authorized disclosures of personal information. The customer is responsible that personal information is collected consistent with the entity's objectives related to privacy. The customer is responsible for corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required. For denied request for correction the customer will inform to data subjects of the denial and reason for such denial. The customer is responsible for provides to the data subjects an accounting of the personal information held and disclosure of a data subject's personal information, upon the data subject's request, consistent with the entity's privacy commitments and system requirements. The customer is responsible for collects and maintains accurate, up-to-date, complete, and relevant personal information. The customer is responsible to implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy.	P1.1 P2.0 P2.1 P3.1 P5.2 P6.1 P6.2 P6.8 P7.1 P8.1

****