Service Organization Controls 3

Report

For the Period from October 1st, 2016 to September 30th, 2017

Report on the Walkme Interactive Online Guidance System Relevant to Security, Availability and Confidentiality

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

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

Fahn Kanne
Grant Thornton

Report of Independent Service Auditors

To the Management of Walkme:

We have examined management's assertion that Walkme, during the period October 1, 2016 through September 30, 2017 maintained effective controls to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification
- the System was available for operation and use, as committed or agreed
- information within the System designated as confidential is protected as committed or agreed

Based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of Walkme's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Walkme's relevant to security, availability and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, Walkme's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability and confidentiality.

February 12, 2018
Tel Aviv, Israel

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

Walkme maintained effective controls over the security, availability and confidentiality of its Interactive Online Guidance System ("System") to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification
- the System was available for operation and use, as committed or agreed
- information within the System designated as confidential is protected as committed or agreed

During the period October 1, 2016 to September 30, 2017, based on the criteria for security, availability and confidentiality in the AICPA's TSP Section 100, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Our attached System Description of the System summarizes those aspects of the system covered by our assertion.

February 12, 2018

DocuSigned by:
Dan Adika
51F3AEF4CEF4436...

Dan Adika
CEO

Description of Walkme Interactive Online Guidance System

Company Overview and Background

WalkMe (the company) enables online businesses and service providers to increase conversion and improve service, while slashing the cost required for supporting customers. The company helps users navigate the features of other web-based services.

Products and Services

WalkMe is a cloud-based Enterprise Class Guidance and Engagement Platform. The context-intelligent Platform guides users and drives them to action within any online experience. The Platform anticipates user needs and provides help exactly when and where they need it. WalkMe also drives users to action by highlighting new features and recommending relevant high-value offerings. All of this is accomplished without any changes to or integration with the underlying software. WalkMe includes three modules: WalkMe Player, WalkMe Editor and WalkMe Insights.

WalkMe uses Amazon Web Services LLC ("AWS") to provide infrastructure management services, GoodData for analytics services, Akamai for CDN and Web Application Firewall services and Logz.IO for logging system.

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).

WalkMe includes three main modules:

- WalkMe Editor: The back-end where your WalkMe admin will create, edit, and publish WalkMe apps
- WalkMe Player: The front-end where your users will access WalkMe apps
- WalkMe Insights: A powerful tool for making sense of how your end-users are experiencing your internal and external online and mobile environment.

.

Components of the system providing the defined services

Walkme policies relevant to Information Security Availability and Confidentiality
The control environment sets the tone of an organization, influencing the control consciousness of its employees. It reflects the overall attitude, awareness, and actions of management, the board of directors, and others, concerning the importance of controls and the emphasis given to controls in the entity's policies, procedures, methods and organizational structure. WalkMe's executive management recognizes its responsibility for directing and controlling operations and for establishing, communicating and monitoring control policies and procedures.

Authority and Responsibility: Lines of authority and responsibility are clearly established throughout the organization and are communicated through WalkMe's:

- management operating style
- organizational structure
- employee job descriptions
- organizational policies and procedures.

Human Resources Policy and Practices: The head of the Human Resources (HR) department is responsible for enabling WalkMe's business needs while creating a productive work environment, as well as enriching and preserving our employees.
The main areas of responsibility include: compensation and benefits, training and development, employee relations, employee engagement and retention, internal communication, talent acquisition and employer branding.

Security and Logical Access
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 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.

User names 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. These settings include: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of unsuccessful attempts to enter a password before the user ID is suspended, and (4) password complexity. Due to system limitations, some configuration parameters may not be available on certain systems. 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 DevOps 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 AWS. 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 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.

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 DevOps team.

Monitoring

WalkMe security, availability and confidentiality performance, as well as potential impairments to the company's ongoing ability to achieve its objectives, are periodically reviewed and compared with the defined system security policies during a semi-annual meeting involving WalkMe management

Support and Operations

WalkMe provides technical support 24 hours a day, 7 days a week, 365 days a year. The Support process consists of three tiers and is designed to enable internally identified issues related to clients and requests raised by clients and internal parties to be handled and resolved. Further description of the Support department is included in the description of controls.

Application backup and restore

WalkMe DevOps 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 DevOps team performs a restoration test from an application database backup to determine that data can be recovered efficiently and in a controlled manner.

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.

****