CYBERARK®

CyberArk Software Ltd.

SOC 3 Type 2

January 1, 2022 to December 31, 2022

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

January 1, 2022 to December 31, 2022

Table of Contents

SECTION 1

ASSERTION OF CYBERARK SOFTWARE LTD. MANAGEMENT

ASSERTION OF CYBERARK SOFTWARE LTD. MANAGEMENT

January 6, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within CyberArk Software Ltd.'s ('CyberArk' or 'the Company') Identity Services System throughout the period January 1, 2022 to December 31, 2022, to provide reasonable assurance that CyberArk's service commitments and system requirements relevant to Security, Availability, and Confidentiality (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "CyberArk Software Ltd.'s Description of Its Identity Services System throughout the period January 1, 2022 to December 31, 2022" 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 January 1, 2022 to December 31, 2022, to provide reasonable assurance that CyberArk's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). CyberArk's objectives for the system in applying 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 "CyberArk Software Ltd.'s Description of Its Identity Services System throughout the period January 1, 2022 to December 31, 2022".

CyberArk uses Amazon Web Services ('AWS' or 'subservice organization') 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 CyberArk, to achieve CyberArk's service commitments and system requirements based on the applicable trust services criteria. The description presents CyberArk's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CyberArk's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve CyberArk's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of CyberArk'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 January 1, 2022 to December 31, 2022 to provide reasonable assurance that CyberArk's service commitments and system requirements were achieved based on the applicable trust services criteria.

_____
Peretz Regev
Chief Product Officer
CyberArk Software Ltd.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To CyberArk Software Ltd.:

Scope

We have examined CyberArk Software Ltd.'s ('CyberArk' or 'the Company') accompanying description of Identity Services System titled "CyberArk Software Ltd.'s Description of Its Identity Services System throughout the period January 1, 2022 to December 31, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2022 to December 31, 2022, to provide reasonable assurance that CyberArk's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CyberArk, to achieve CyberArk's service commitments and system requirements based on the applicable trust services criteria. The description presents CyberArk's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of CyberArk's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, 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 CyberArk, to achieve CyberArk's service commitments and system requirements based on the applicable trust services criteria. The description presents CyberArk's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of CyberArk'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

CyberArk 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 CyberArk's service commitments and system requirements were achieved. CyberArk has provided the accompanying assertion titled "Assertion of CyberArk Software Ltd. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. CyberArk is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:
- 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 the description is presented in accordance with the description criteria
- 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
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 CyberArk's Identity Services System were suitably designed and operating effectively throughout the period January 1, 2022 to December 31, 2022, to provide reasonable assurance that CyberArk's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on CyberArk'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 CyberArk, user entities of CyberArk's Identity Services during some or all of the period January 1, 2022 to December 31, 2022, business partners of CyberArk subject to risks arising from interactions with the Identity Services, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization 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
January 6, 2023

SECTION 3

**CYBERARK SOFTWARE LTD.'S DESCRIPTION OF ITS CYBERARK
IDENTITY SERVICES SYSTEM THROUGHOUT THE PERIOD
JANUARY 1, 2022 TO DECEMBER 31, 2022**

OVERVIEW OF OPERATIONS

Company Background

CyberArk is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security offering for any identity - human or machine - across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle. The world's leading organizations trust CyberArk to help secure their most critical assets.

Description of Services Provided

CyberArk Workforce Identity helps today's businesses overcome the unique user authentication, authorization, and auditing challenges accompanying digital transformation. The services included in CyberArk Identity solution streamline operations and gives workers simple and secure access to all their enterprise resources-on-premises, cloud, hybrid-from any location, using any device.

The integrated CyberArk Identity solution includes:
- CyberArk Identity Single Sign-On (SSO): gives workers convenient one-click access to all their enterprise applications using a single set of credentials. The solution helps eliminate password sprawl and fatigue, improve user experiences, and avoid risky workarounds like using common credentials, or recording passwords on paper or spreadsheets. The solution also centralizes, unifies, and simplifies access administration, reducing help desk interactions and operations expenses
- CyberArk Identity Adaptive Multi-Factor Authentication (MFA): helps businesses avoid data loss and other risks posed by compromised or stolen credentials. The solution supports a variety of authentication mechanisms, including passwordless factors, and protects a range of enterprise identities and resources, such as applications, infrastructure, and endpoints. Unlike traditional MFA solutions, CyberArk Identity Adaptive MFA uses AI-powered behavioral analytics and contextual information to determine which authentication factors to apply to a particular user in a specific situation, improving end-user satisfaction and productivity
- CyberArk Identity Lifecycle Management (LCM): lets administrators efficiently onboard and offboard users and manage their access privileges throughout their course of employment. The solution includes self-service tools for users and approving managers, as well as administrative reports to help security teams track access activity, investigate incidents, and support compliance audits. Integration with leading HR systems, Identity Governance and Administration solutions, and directory services simplifies new-hire provisioning and eliminates manually-intensive, error-prone processes
- CyberArk Identity App Gateway: lets users securely access traditional applications hosted in corporate data centers using the same credentials and authentication methods they use to access cloud apps. The solution provides strong security and easy access without VPN hassles, expenses, or support burdens. Easy to implement, CyberArk Identity App Gateway can be deployed without modifying application code or reconfiguring firewall rules
- CyberArk Identity Secure Web Sessions: records, audits and protects end-user activity within designated web applications. The solution uses a browser extension on an end-user's endpoint to monitor and segregate web apps that are accessed through CyberArk Identity Single Sign-On (SSO) and deemed sensitive by business application owners, enterprise IT and security administrators. Security and compliance professionals can use Secure Web Sessions to efficiently identify anomalous activity, investigate issues and support audits
- CyberArk Identity Directory Services: lets organizations centrally manage enterprise IT directories at scale. The solution integrates with a variety of popular on-premises and cloud-based directory services including Microsoft Active Directory, Azure Active Directory, and LDAP Directories. An extensible schema makes it easy to maintain information related to users, computers, endpoints, mobile and server objects, and other elements using a unified data store and common administrative tools

- CyberArk Identity User Behavior Analytics: uses AI and Machine Learning to collect, analyze, and visualize user behavior and threat data in real-time. The solution includes interactive dashboards to help administrators easily assess risk, reporting tools to help administrators investigate security incidents and support audits, and real-time alerts to notify administrators of suspicious activity. It also provides webhooks to feed alerts to third-party tools like ServiceNow
- The Workforce Password Management capability enables companies to securely store and manage password-based credentials and other non-web-app items in CyberArk Cloud or optionally self-hosted CyberArk Vault and enforce robust controls over business application access. It also provides users seamless; one-click access to business apps and eliminates the need to save credentials in password managers or browsers
- CyberArk Identity Flows allows organizations to eliminate manual tasks and processes by automating complex identity management workflows. A no-code visual editor and thousands of pre-built connectors make it possible to rapidly orchestrate identity events, build workflows, and synchronize identity data across diverse applications, directory stores, and repositories

Principal Service Commitments and System Requirements

CyberArk designs its processes and procedures related to the Identity Platform to meet its objectives for its Identity Platform. Those objectives are based on the service commitments that CyberArk makes to user entities, the laws and regulations that govern the provision of Identity Platform SaaS service, and the financial, operational, and compliance requirements that CyberArk has established for the service. The Identity Platform SaaS solution of CyberArk are subject to the security and privacy requirements of the relevant privacy and security laws and regulations in the jurisdictions in which CyberArk operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:
- Security principles within the fundamental designs of the Identity Platform that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role
- Use of encryption technologies to protect customer data both at rest and in transit

CyberArk establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in CyberArk's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Identity Platform.

Components of the System

Infrastructure

Primary infrastructure used to provide CyberArk's Identity Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS Aurora Postgres	Postgres	Customer data storage -Identity Services
AWS Redshift	Not applicable	Customer data storage - Analytics Services
AWS EC2	Windows, Linux	Compute

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS S3	Not applicable	Log Management

Software

Primary software used to provide CyberArk's Identity Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Dynatrace, Cloud Watch	Linux	Application monitoring
AWS Aurora Postgres DB - RDS snapshots	Not applicable	Backup/Replication
ELK/AWS S3	Not applicable	Logging/Storage
PagerDuty	Not applicable	Infrastructure monitoring/Alerting
Checkmarx	Windows Server 2016	Vulnerability and Patch management
Symantec	Windows Server 2016	Anti-virus
JIRA	Not applicable	Helpdesk/Ticketing system

People

CyberArk staff provides support for the above services in each of the following functional areas:
- Executive management - provides general oversight and strategic planning of operations
- Development team - responsible for delivering a responsive system that fully complies with the functional specification
- Quality assurance team - verifies that the system complies with the functional specification through functional testing procedures
- System administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Customer data is captured which is utilized by CyberArk in delivering its Identity Platform. Such data includes, but is not limited to, the following:
- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, IDS alerts, or automated patching systems

Processes, Policies and Procedures

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

Physical Security

Employees are provided with a card access and granted access to CyberArk Offices as defined by their roles. The access card/ID system is used to control access in order to enter an office. Certain areas are more sensitive than others and require extra security. Visitors in CyberArk Offices must be escorted and follow the company guidelines beyond the entrance point. Visitors must present a clearly visible visitor badge. Upon an employee's termination of employment, the access is disabled form the facility. The Chief Information Security Officer (CISO) is responsible for assessing and providing physical security solutions to all CyberArk Offices globally.

The CyberArk Identity solution runs on AWS datacenters which are Service Organization Control (SOC) 2 Type II certified, with fully redundant power backup systems, fire suppression systems, and security guards. All datacenters are hardened against physical intrusion, and server room access is limited to certified employees.

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system.

Logical Access

CyberArk uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. The procedures include the life cycle of user access from the initial registration to de registration of users who no longer need access. Resources are protected using native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. Segregation of duty is in place between the group who approves the access and the group that provides the access.

Asset management procedures are in place to define the process of receiving, tagging, documenting and disposing of the equipment's. An information security steering committee consisting of the Chief Executive Officer (CEO), General Manager (GM), Chief Information Officer (CIO) and CISO hold regular meetings to review the information security projects and other necessary management activities.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completions. Business related data is protected by regular backups performed per the schedule. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately. The IT department practices procedures to store information to prevent unauthorized use. Regular restores are performed certain defined files.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

CyberArk monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements.

CyberArk 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:
- Data center space, power and cooling
- Disk storage
- Network bandwidth

CyberArk has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. CyberArk's business continuity plan and disaster recovery plans are designed to provide solutions in case of disasters and unexpected interruptions.

<u>Change Control</u>

CyberArk maintains documented change management policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing results are maintained for the changes. Development and testing are performed in an environment that is logically separated from the production environment. Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

<u>Data Communications</u>

Firewall systems 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 Internet Protocol (IP) addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that 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 to measure the security posture of a target system or environment. Vulnerability scanning is performed as a part of the penetration testing. Authorized employees may access the system through from the Internet through the use of Virtual Private Network (VPN) technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Boundaries of the System

The scope of this report includes CyberArk's Identity Services System performed at the Newton, Massachusetts (United States headquarters), Tel Aviv, Israel (corporate headquarters) and various other locations by personnel working remotely.

This report does not include the cloud hosting services provided by AWS performed at various facilities.

Changes to the System in the Last 12 Months

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

Incidents in the Last 12 Months

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

Criteria Not Applicable to the System

All Common Criteria / Security, Availability, and Confidentiality criteria were applicable to the CyberArk's Identity Services System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at various facilities.

Subservice Description of Services

CyberArk leverages a variety of AWS offerings for hosting CyberArk platform infrastructure. AWS allows for a secure, scalable and redundant utilization of cloud compute, storage and network resources. Listing of utilized AWS services is detailed under "Components of the System: Infrastructure" section of this document.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the control objectives described within this report are met:

Subservice Organization - Amazon Web Services		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Common Criteria / Security, Confidentiality	CC6.5, C1.2	All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.
		AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.
		AWS retains customer content per customer agreements.

Subservice Organization - Amazon Web Services		
Category	**Criteria**	**Control**
Common Criteria / Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		S3-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		S3-Specific - Objects are stored redundantly across multiple fault-isolated facilities.
		S3-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		RDS-Specific - If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.

CyberArk management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, CyberArk performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and the subservice organization

- Monitoring external communications, relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

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

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 CyberArk.
2. User entities are responsible for notifying CyberArk of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of CyberArk services by their personnel.
5. User entities are responsible for providing CyberArk with a list of approvers for security and system configuration changes for data transmission.
6. User entities are responsible for immediately notifying CyberArk of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
7. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize CyberArk services.
8. User entities are responsible for user access administration in the CyberArk SaaS product, including reviewing access for their personnel as needed.
9. User entities are responsible for exporting any customer data from the SaaS product to which they desire continued access to within 60 days of termination or expiration of the customer's subscription term.