CYBERARK®

Safeguarding Privileged Access

Implementing ISO/IEC 27002 Security Controls with the CyberArk Solution

Contents

Executive Summary

Meeting an Internationally-Recognized Information Security Standard

Given the escalation of cyber-attacks, many organizations worldwide are intensifying efforts to protect valuable information assets such as customer data and intellectual property. Governments and industries in many countries continue to add new regulations and strengthen existing rules mandating data protection. Often the regulations don't offer specific requirements but call for organizations to follow standards of best practice. Increasingly, customers and business partners are adding more stringent requirements to contracts and expecting their vendors and service providers to substantiate their information security practices, further encouraging organizations to use standards.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27002 standard is an internationally acclaimed standard of best practice for information security. Many organizations globally use the standard as part of their information security program. For large global enterprises that operate in multiple countries, it can be useful as a general controls framework to help achieve compliance with many country-specific regulations. For small-to-medium sized companies, it can be an effective tool in establishing more mature information security controls.

Following an internationally-recognized standard helps organizations to meet contractual obligations with customers and business partners. For service providers, from cloud data centers to law offices, their license to operate increasingly requires them to prove they are responsible stewards of sensitive information for a global clientele. Auditors worldwide also rely on ISO 27002 as a basis for evaluating controls and/or verifying compliance to various regulations and standards.

ISO/IEC Standards for Information Security

The ISO/IEC 27000-series provides best practice recommendations for information security, including various aspects such as risk assessment, controls implementation, and incident response, within the context of an overall information security management system (ISMS).

The flagship standards are the ISO/IEC 27001, which defines the mandatory requirements for an "Information Security Management System (ISMS)" and its companion, the ISO/IEC 27002 standard, entitled "Information technology — Security techniques — Code of practice for information security controls. The latest versions of these standards, ISO/IEC 27001:2013 and ISO/IEC 27002:2013, were published October 1, 2013.

Organizations can choose to use these standards as a general framework for best practices or become officially certified. If they choose the certification route, organizations work with an accredited certification body to become certified against the ISO/IEC 27001 standard. ISO/IEC 27002 outlines the set of recommended controls that can be applied. Each organization also determines the scope of implementation. For example, they might adopt ISO 27002 globally in selecting security controls for all information systems worldwide across their extended enterprise or apply it at a local-level for particular data centers in certain geographic locations.

Prioritizing on Privilege

The ISO/IEC 27002 standard makes recommendations for a comprehensive suite of information security controls. It recognizes that the resources used in implementing controls need to be balanced against the risks. In adopting the ISO/IEC 27002 standard, a focus area for many organizations is improving the implementation of controls for protecting privileged accounts. With powerful access rights, privileged accounts are basically the organization's "keys to the IT kingdom." Privileged accounts consist not only of information system administrator or super-user accounts but also select business users, social media accounts and are found hard-coded in virtually every piece of hardware and software across an organization.

With sophisticated attacks on the rise, insecure privileged accounts represent a serious vulnerability. It is well-known that rogue insiders and external attackers go after privileged accounts as part of their modus operandi. Compromised privileged credentials have been used in attacks to steal millions of credit card records, exfiltrate multiple years' worth of R&D, expose confidential national security data, and more. Another growing concern is third-party risk, as increasingly cyber-attackers target privileged credentials at smaller service providers in order to gain entry into larger organizations.

ISO/IEC 27002 Emphasis on Safeguarding Privileged Access

Considering the potential risks, it's understandable that ISO/IEC 27002:2013 contains substantial guidance regarding safeguarding privileged access. It warns that "the inappropriate use of system administrator privileges... is a major contributory factor to failures or breaches of systems."[1] The standard calls on organizations to pay particular attention to privileged user accounts, given their abilities to override system or application controls, make unauthorized changes to operational software, or manipulate the logs on information systems, and so on.

ISO/IEC 27002 contains a broad-range of controls related to safeguarding privileged access.

Organizations are advised to implement the necessary controls to reduce the risk of unauthorized use of privileges. The recommendations stress the importance of managing privileged access rights in order to protect information. For example, in cases of termination or resignation, disgruntled employees or contractors can use their privileged access rights to deliberately corrupt or sabotage information; and/or be tempted to collect information for future use.

There are controls related to securing privileged accounts throughout the ISO/IEC 27002:2013 standard, including requirements for:

- Establishing and implementing privileged access policy
- Identifying the privileged access rights associated with each system or process
- Restricting the use of privileged access to authorized users based on functional roles
- Authenticating privileged users, ensuring individual accountability for privileged actions
- Changing default vendor passwords
- Restricting access to privileged utility programs
- Controlling privileged access by suppliers
- Logging and monitoring privileged access

For a look at some of the key controls related to securing privileged access, see pages 5-7. A complete list can be found on pages 8-20.

[1] "ISO/IEC 27002:2013 pg 22" CyberArk

CyberArk's Comprehensive Approach

As the trusted experts in privileged account security, CyberArk provides a comprehensive approach to help organizations implement security controls to protect privileged access across the organization's IT environment. With the CyberArk Privileged Account Security Solution, organizations can implement effective information security controls to:

- Locate, manage and control all privileged accounts – including full lifecycle management
- Ensure only authorized users have access to privileged accounts
- Protect privileged credentials in CyberArk's patented digital vault with seven layers of security
- Track, monitor and record all privileged activity – to sensitive servers, databases or virtual machines by internal users, applications, and third-parties
- Uniquely identify all administrative users and restrict their use of privileged accounts to necessary job functions
- Ensure vendor-supplied default passwords are changed and automate password changes for all privileged accounts
- Eliminate hard-coded credentials, including passwords and encryption keys from applications, service accounts and scripts with no impact on application performance or business processes
- Analyze, detect and alert on anomalous privileged user behavior – enabling quick response by incident response teams

Quick View: Key Controls Related to Privileged Access

The table below highlights some of the key controls pertaining to privileged access within ISO/IEC 27002:2013 and the key capabilities of CyberArk's solution for implementing those controls. See pages 8 - 20 for a comprehensive list of controls and in-depth explanation of CyberArk's solution's capabilities.

Key ISO Controls related to Privileged Access	Key Capabilities of CyberArk's Privileged Account Security Solution
6.1.2 Segregation of duties	Enables the segregation of duties by restricting access to privileged credentials, for example administrator access can be separated according to technology area. ▪ Organizations can also separate the initiation of an event, such as requesting access to an information asset, from the authorization.
6.2.2 Teleworking	Helps implement security measures for remote privileged access by teleworkers. ▪ A secure zone for all privileged connections can be created so organizations can have full control of who can gain remote access and when, and record and monitor all remote privileged access sessions in real-time.
9.1.1 Access control policy	Features "Master Policy" which delivers unified policy management for all privileged access across an organization's IT environment. ▪ Organizations can implement access control policies operating on "need-to-know" and "need-to-use" principles.

9.1.2 Access to networks and network services	Controls access to the network's privileged credentials. ▪ Access by network admins can be restricted to only the networks and network services to which they are entitled.
9.2.1 User registration and de-registration	Ensures all users, including each person and application, have a unique ID to access privileged credentials within the digital vault. ▪ Organizations can ensure individual accountability - even for administrative accounts that use shared credentials.
9.2.2 User access provisioning	Enables the assignment and revocation of access rights to privileged credentials according to organizational approvals and based on the user's roles or functions. ▪ Information system owners and managers can easily be granted strict control and oversight of access rights.
9.2.3 Management of privileged access rights	Streamlines all of the processes associated with managing privileged credentials across the IT environment. ▪ Organizations can implement and enforce fine-grained least privilege policies and protect against unauthorized use of generic administration user IDs.
9.2.4 Management of secret authentication information of users	Keeps secret authentication information for privileged accounts confidential; users have no knowledge of administrative passwords, including those shared by a group. ▪ Organizations can also effectively and efficiently change all vendor-supplied default passwords and mitigate password vulnerabilities.
9.2.5 Review of user access rights	Centralizes the management of privileged accounts, making it easy for asset owners to frequently review access rights to privileged credentials to ensure that unauthorized privileges have not been obtained.
9.2.6 Removal or adjustment of access rights	Automates the process of removing and adjusting access rights to privileged credentials.
9.3.1 Use of secret authentication information	Eliminates the insecure practice of keeping a paper or digital record of passwords by securely storing privileged credentials in the tamper-proof Digital Vault.
9.4.1 Information access restriction	Provides granular access control restricting the information privileged users can access and what tasks they can perform down to the command level.
9.4.2 Secure log-on procedures	Supports a range of authentication methods, including: passwords, PKI, RADIUS, LDAP, RSA SecurID, Windows authentication, Oracle SSO and a robust infrastructure for integrating with most Web SSO or OTP solutions.

9.4.3 Password management system	Provides centralized password management for all privileged accounts across an IT environment, including managing their complete lifecycle, automating password changes, and ensuring quality passwords.
9.4.4 Use of privileged utility programs	Eliminates hard-coded passwords from utility programs and uses an advanced means to authenticate the programs that are requesting privileged credentials.
12.1.2 Change management	Helps ensure only authorized users gain privileged access to systems they are entitled to change. ▪ Access not granted without an approved and validated change record.
12.2.1 Controls against malware	Isolates, controls and monitors privileged access and activities for critical systems. ▪ By acting as a jump server, the solution provides a single access control point, and prevents malware from jumping to a target system.
12.4.1 Event Logging	Generates a rich set of real-time data on all privileged account activity across an organization's IT environment; and provides centralized logging and recording of all privileged access to systems.
12.4.2 Protection of log information	Protects all logs and session recordings for privileged account activity with CyberArk's patented, ICSA-certified Vaulting Technology® which employs multiple built-in layers of security. CyberArk's tamper-proof digital vault uses AES 256 cryptographic storage and is FIPS 140-2 certified.
15.1.1 Information security policy for supplier relationships	Helps mitigate the risks associated with suppliers' privileged access to the organization's information assets. ▪ Suppliers who remotely request access to the network gain access to the digital vault through a proxy; so their session is encrypted and isolated from the internal network and all of access can be tracked and monitored.
15.1.3 Information and communication technology supply chain	Addresses the risks associated with deploying information and communications technology from an external supplier. ▪ CyberArk is a trusted supplier of privileged account security products to organizations worldwide.
18.2.3 Technical compliance review	Provides centralized policy management and reporting for all privileged access across an organization, enabling regular review for compliance to the security policy.

Controls Mapping

How CyberArk Helps Implement ISO/IEC 27002:2013 Controls Related to Privileged Access

The following table details how the CyberArk Privileged Account Security solution helps organizations to implement the full range of controls pertaining to privileged access within the ISO/IEC 27002:2013 standard.

NOTE: The list of controls is provided as general summary information only and limited to a subset of the controls - those pertaining to privileged access. Organizations should refer to the ISO/IEC 27002:2013 publication for comprehensive guidance on the complete set of controls. Explanations regarding the CyberArk solution and how it can help organizations to implement the controls pertaining to privileged access are also provided as general summary information only. Organizations must work with information security auditors or ISO standard certification bodies to determine if their particular security controls meet the requirements of the ISO/IEC 27002:2013 standard.

ISO Control	CyberArk Privileged Account Security Solution Capabilities
5.1.1 Policies for information security	CyberArk's "Master Policy" provides unified policy management for all privileged access across an organization's IT environment. The solution provides a policy engine to simplify the process of transforming written policy and procedures into technical settings for operational departments. It enables organizations to accurately enforce policy and quickly implement controls for privileged account security. The policy can be easily managed and understood by employees (e.g. security operations and risk teams) and relevant external parties (e.g. auditors). Organizations can set global policy while providing controlled, granular level exceptions to meet the unique operational needs of the business
6.1.2 Segregation of duties	The CyberArk solution supports the segregation of duties by restricting privileged access to information assets. Access is restricted by controlling access to privileged account passwords stored securely within the CyberArk patented Digital Vault™. For example, the solution can separate administrative access by technology area such as restricting network admins to network devices and Windows admins to Windows servers. Individual privileged users can be assigned specific command-level privileges based on their roles. As well, the initiation of an event, such as requesting access to an information asset, can be separated from the authorization. "Dual Control" can specify that access to highly sensitive passwords requires confirmation by one or more authorized users. Once a user has been granted privileged access to an information asset, the solution can record all actions performed using the privileged credential. Organizations can effectively implement automated controls for controlling and monitoring privileged users so that no single person can access, modify or use assets without authorization or detection.

6.2.2 Teleworking

With the CyberArk solution, organizations can enforce policy and implement security measures for remote privileged access by teleworkers such as administrative staff, contractors, or outsourcers.

A secure zone for privileged connections can be created, enabling full control of who can gain remote access and when, and the recording and monitoring of all remote access sessions in real-time. A range of authentication methods for remote access is supported including: passwords, PKI, tokens, OTP solutions, and smart cards. The solution provides enforcement of workflows such as managerial approval, ticketing integration, session duration limitation and automatic termination when idle.

8.1.3 Acceptable use of assets

The CyberArk solution enables organizations to provide notifications to users requesting privileged access to information assets, informing them of acceptable use and security requirements. During the login procedure, a message can be displayed which requires the user to agree to the terms and conditions of privileged access. Once the user has agreed, they are connected to the system, at which point another message can provide more information including the expectation of recording and monitoring of privileged sessions.

9.1.1 Access control policy

For establishing an access control policy, the CyberArk solution's "Master Policy" provides unified policy management for all privileged access across an organization's IT environment. For more info see 5.1.1.

The solution supports the deployment of role-based controls for privileged access, helping organizations to implement access control policy operating on "need-to-know" and "need-to-use" principles. Organizations can also ensure that all privileged access not explicitly allowed by the policy is denied.

9.1.2 Access to networks and network services

To protect privileged access to networks and network services, the CyberArk solution restricts access to the network's privileged credentials. Access by network admins can be restricted to only the networks and network services to which they are entitled. For example, global organizations can restrict access to networks geographically, such as allowing only U.S. admins access to the U.S. network, etc. Organizations can also control the network address (e.g. only from the office) and the protocol (e.g. SSH) used to connect to the target system

A range of two-factor authentication methods can be used to access the privileged credentials in the digital vault, including: PKI, tokens, OTP solutions, and smart cards. The solution enables the recording of privileged activities on the network and monitoring sessions in real-time.

9.2.1 User registration and de-registration

For managing privileged access, the CyberArk solution supports the implementation of a registration and de-registration process. All users must have a unique ID to access privileged credentials within the CyberArk patented Digital Vault, including each person and application, ensuring individual accountability.

For administrative accounts where it is often necessary to use shared credentials - such as Administrator on a Windows server, Root on a UNIX server, or Cisco Enable on a Cisco device - the solution mitigates the inherent risks and removes the difficulties in ensuring individual accountability. To retrieve the shared administrative credential, authorized administrators must use a unique user ID and authentication method to login into the digital vault. The unique identity of the administrator is linked to their use of the shared credential. All actions performed using the shared credential can be recorded and monitored in real-time, ensuring that individual users can be held responsible for their actions, even when there are multiple users using the same shared credential to perform different tasks at the same time.

Furthermore, administrators have no knowledge of the shared passwords, greatly reducing the risk of exposure. The shared credential is stored securely within the digital vault. Organizations can centrally secure, manage and track the use of all shared credentials across their IT environment.

The CyberArk solution helps organizations to ensure the validity of user IDs used for privileged access by seamlessly integrating with enterprise directories. Through LDAP integration, any account changes – including deletion of user IDs – is automatically propagated to the account information held in the vault. Upon termination, once a user is removed from the directory, their privileged access is immediately revoked. As well, any inactive privileged accounts removed from the directory are automatically removed from the vault.

9.2.2 User access provisioning

The CyberArk solution facilitates the implementation of a formal provisioning process for privileged access. Organizations can centralize privileged account management for all users such as administrators and applications and maintain a central record of access rights to privileged credentials, which are securely stored in the digital vault.

The solution enables the assignment and revocation of access rights to privileged credentials according to organizational approvals and based on the user's roles or functions. Information system owners and managers can easily be granted strict control and oversight of credential access rights through the solution's seamless approvals process. They can also add or remove credential access rights for specific users or sets of users on the fly as requirements change, for fast and efficient provisioning/de-provisioning.

Customizable "request workflows" for credential access approval is provided, such as integration with helpdesk ticketing systems and a "two-person rule" feature. Dual Control is a need-based workflow that functions as a two-person approval and verification system for privileged access. For specific sensitive data or systems, when authorized users request access to credentials, the request can be instantly relayed to data owners, empowering them to approve or deny access on a case-by-case basis.

Organizations can easily adapt or remove access rights to privileged credentials for users who change roles or leave the organization. Team managers can define access rights for their particular workgroup, facilitated by the use of safes within the vault. For establishing conditions for group or role membership, organizations can leverage the group structure already created in their LDAP database such as Active Directory. As well, if a user is removed from the directory, their access to privileged credentials is immediately revoked.

9.2.3 Management of privileged access rights

For the management of privileged access rights, CyberArk's automated solution enables organizations to control all of the processes associated with using privileged credentials across the IT environment. Out-of-the-box credential management is provided for over 100 operating systems, databases, firewalls, network devices, virtual machines, websites, and cloud-based applications. Extensible support for additional systems is provided with unique plug-in architecture for fast integration.

To help organizations identify all of their privileged accounts, the CyberArk solution provides an automatic discovery tool. With a clear record of all service accounts, devices, and applications, organizations can achieve a true understanding of the size and magnitude of their privileged account security risk. Discovery and provisioning of accounts ensures that even accounts hidden in services, scheduled tasks, application pools or local administrator groups are discovered and managed securely according to organizational policy.

Organizations can allocate access rights to privileged credentials on a need-to-use basis and on an event-by-event basis, restricting users to the least privileges necessary for their functional roles. The solution supports the implementation and enforcement of fine-grained least privilege policies; users can only access the particular privileged IDs to which they have been granted access and therefore only perform tasks that are assigned to that privileged ID. Individual authorized users can be assigned specific command-level privileges based on their roles.

As indicated in 9.2.2. CyberArk provides an extensive authorization process and centralized record of all access rights to privileged credentials. Organizations can also ensure that privileged credentials are used only for privileged activities. Privileged credentials can be set up with time limitations and automatic expiry.

The CyberArk solution also protects organizations from the unauthorized use of generic administration user IDs. The confidentiality of the secret authentication information is maintained; administrators have no knowledge of privileged passwords for generic accounts. Furthermore, password changes can be automated based on an organizationally-defined time-frame, enabling organizations to schedule password changes including after every use. Authorized administrators must use a unique user ID and password to login to the digital vault and gain access to the administrative account. The unique identity of the administrator is linked to their use of the privileged credential. All actions performed using the privileged credential can be recorded and monitored in real-time, ensuring that individual users can be held responsible for their actions.

9.2.4 Management of secret authentication information of users

With CyberArk's automated solution, organizations can implement a formal management process for the allocation of secret authentication information for privileged accounts. It provides password management for the entire lifecycle of privileged accounts across the IT environment.

All secret authentication information for privileged accounts is kept confidential; users have no knowledge of administrative passwords, including passwords shared by a group. In fact, with automated password changes, it is possible that no one in the organization knows the secret authentication information for any privileged credential. All privileged account information is stored in encrypted format in the digital vault.

Using the CyberArk solution, organizations can effectively and efficiently change all vendor-supplied default passwords and mitigate password vulnerabilities for every piece of software and hardware throughout an IT environment. The solution replaces insecure practices such as the use of repeat and static passwords with a system that automatically generates unique passwords and meets password strength and refresh requirements defined by organizational policy.

9.2.5 Review of user access rights

By centralizing the management of privileged accounts, the CyberArk solution makes it easy for asset owners to frequently review access rights to privileged credentials to ensure that unauthorized privileges have not been obtained. For systems protected with the CyberArk solution, organizations can record any privileged sessions involving changes to privileged credentials, such as creating new accounts or elevating privileges. The actions can be recorded for periodic review or monitored in real-time. The solution also provides extensive logging of privileged credential changes such as tracking when users are added to groups, which helps determine if a new member inadvertently gains excessive access rights to privileged credentials.

9.2.6 Removal or adjustment of access rights

The CyberArk solution automates the process of removing and adjusting access rights to privileged credentials. Through LDAP integration, any changes to a user account – including modification of a user's role or deletion of user ID – are automatically propagated to the account information held in the digital vault. When an employee is terminated or an external party's contract expires, once these users are removed from the directory, all access to privileged credentials is immediately revoked.

To address the need to reissue shared/group account credentials, the solution can be set up to automatically notify account administrators when an individual is removed from a group in LDAP and enable them to immediately change the shared/group password. However, typically the shared/group password is never disclosed to users and it is automatically refreshed on a regular basis, making it unnecessary to change the password. To ensure access is removed upon termination of employment or contract, the organization can specify a time period for which employees or external parties are allowed access to the credentials in the digital vault, automatically removing access after the allotted time period.

9.3.1 Use of secret authentication information

With the CyberArk solution, typically privileged passwords are never disclosed to users, eliminating the insecure practice of keeping a paper or digital record. The solution provides centralized password management for all privileged accounts across an organization including automated password selection and changes. See 9.4.3 for more information.

The CyberArk solution also ensures proper protection of passwords; all privileged account information is stored using CyberArk's patented ICSA-certified Vaulting Technology®, which employs multiple built-in layers of security. All privileged passwords are protected with strong AES 256 encryption both in transit and at rest. As well, privileged credentials in the digital vault can be accessed with a range of authentication methods, including: passwords, PKI, RADIUS, LDAP, RSA SecurID, Windows authentication, Oracle SSO and a robust infrastructure for integrating with most Web SSO or OTP solutions.

9.4.1 Information access restriction

The CyberArk solution enables organizations to restrict privileged access to information and application system functions. Particular users requiring privileged access can be limited to accessing specific data or applications, or to performing certain tasks such as read, write, delete and execute. With granular access control, organizations can control and monitor what privileged users can do down to the command level.

9.4.2 Secure log-on procedures

To help organizations control privileged access to systems and applications, the CyberArk solution supports the implementation of secure log-on procedures.

To log-on to systems and applications, users must access privileged credentials in the digital vault. The solution supports a range of authentication methods, including: passwords, PKI, RADIUS, LDAP, RSA SecurID, Windows authentication, Oracle SSO and a robust infrastructure for integrating with most Web SSO or OTP solutions.

Organizations can configure the log-on to display a general notice warning that access to the system or application is limited to authorized users. The log-on process can also display information upon completion of a successful log-on, such as number of previous failed log-on attempts since the last successful login.

The solution supports the implementation of the full range of secure log-on procedures such as not displaying users' passwords while they are authenticating to the vault, not using help messages which reveal log-on information; and validating log-on information only on completion of all input data. For transmitting privileged passwords over a network, the CyberArk solution uses strong AES 256 encryption.

Organizations can protect against brute-force log-on attacks by limiting repeated access attempts. Users who fail authentication to the vault are locked out until enabled by an administrator, preventing access to privileged credentials. Re-authentication for users or applications can be required based on inactivity or time-limits. Privileged session connection times can be restricted to certain times of day and sessions can be disconnected when a threshold (i.e. 15 minutes) is reached.

Application access can also be protected against (for example) brute-force log-on attacks. To perform designated tasks like processing information in a database, applications must be granted use of privileged accounts. Credentials are typically hard-coded and in clear text within applications, making them susceptible to brute-force attacks. Instead, the CyberArk solution effectively eliminates embedded application credentials. For example, to access a database, an application must first have authorized access to the privileged credential in the vault. To gain access to the credential, an application is authenticated using advanced authentication methods, based not only on ID and password but also on specific application characteristics including the server it resides on, the operating system it uses, and a crypto "fingerprint." Organizations can ensure only authorized applications with the appropriate ID and characteristics can access the database.

The CyberArk solution can record and monitor all access attempts to privileged credentials in the digital vault. All valid and invalid access attempts by privileged credentials can also be logged, such as an application attempting to connect to a database.

For raising security events such as a potential attack on log-on controls, the CyberArk solution integrates with Security Information and Event Management (SIEM) and event log systems. In addition, CyberArk Privileged Threat Analytics enables organizations to compare real-time to historical log-on activity for privileged accounts in order to detect anomalies as they occur. For example the solution would detect if a user is attempting to access privileged credentials outside of their authorized working hours.

9.4.3 Password management system

For privileged accounts, the CyberArk solution provides complete password management, enabling organizations to automate and secure all of the processes associated with using privileged credentials and managing their lifecycle, including ensuring quality passwords.

The CyberArk solution helps organizations enforce the use of individual user IDs for all privileged access throughout their IT environment. For more information on ensuring users are uniquely identified and held accountable, see 9.2.1.

The solution includes flexible and centralized password management for all privileged accounts across an organization. Organizations can set policy for privileged password format, including the requirements for a minimum length, and numeric and alphabetic characters; and can ensure passwords are unique and not reused. Changes to privileged passwords can be done manually whenever needed or automated based on an organizationally-defined time-frame, enabling organizations to schedule password changes including after every use, and to enforce time limitations on passwords.

Privileged passwords are stored using CyberArk's patented ICSA-certified Vaulting Technology, which employs multiple built-in layers of security to protect privileged credentials. With the CyberArk solution, all privileged passwords are protected with strong AES 256 encryption both in transit and at rest.

9.4.4 Use of privileged utility programs

The CyberArk solution enables organizations to restrict access to privileged utility programs and control utility program access to systems and applications, by controlling access to the privileged account credentials stored securely in the digital vault. Access can be restricted to a certain time period and can be disabled when not in use. "Dual Control" can specify that access to highly sensitive credentials requires confirmation by one or more authorized users. As well, administrators can be granted authorized access to resources but never see the privileged account password in clear text.

Many utility programs involve the use of service accounts; services such as back-up or vulnerability scanning require privileged access to systems. To perform their designated tasks such as retrieve, process, transmit and store sensitive data, these programs require high levels of access to running processes. Service accounts are difficult to secure since the credentials are typically hard-coded and in clear text within the programs. The CyberArk solution eliminates hard-coded passwords from utility programs and uses an advanced means to authenticate the programs that are requesting credentials. Access is granted only to trusted programs, with no impact to performance or downtime.

The solution provides a tamper-proof audit record to track all privileged account access to utility programs and all utility program service account access to systems.

9.4.5 Access control to program source code.

To restrict access to program source code, the CyberArk solution helps organizations by ensuring only authorized users gain access to development environments. See 14.2.6 for more information.

10.1.2 Key management

The CyberArk solution supports detection, the protection, and management of cryptographic keys used for authenticating privileged users and applications and for establishing privileged sessions. The solution provides a secure cryptographic SSH key management system including complete lifecycle management

Key management features include:

- Key storage
  - Stores and fully protects private keys centrally in the digital vault.
  - Enables definition of access controls and levels of authorization (e.g. use private key, retrieve private key, change private key …)
- Key rotation and verification
  - Rotates SSH keys periodically or on-demand, verifying that the SSH key pair is still valid.
  - Provides for selection of key type, length, and strength
  - Distributes to target systems after keys are rotated.
- Key archiving
  - Ensures ongoing backup of private keys by storing them in the digital vault.
- Detection of unmanaged keys
  - Detects orphan keys or keys that are not yet managed by the system.
- Logging and Auditing
  - Logs all access to private keys stored in the digital vault.
  - Centralizes logging and auditing of privileged credentials, including SSH keys and passwords.

12.1.2 Change management

To control changes to information systems, the CyberArk solution helps ensure that only authorized users can gain privileged access to systems they are entitled to change. Out-of-the-box integration is provided for over 100 operating systems, databases, firewalls, network devices, virtual machines, websites, and cloud-based applications; with extensible support for additional systems. Unique plug-in architecture supports fast integration.

Access is restricted by controlling access to administrative passwords stored securely in the digital vault. "Dual Control" can specify that access to passwords used to gain entry to highly sensitive systems requires confirmation by one or more authorized users, greatly limiting the ability to make unauthorized changes. As well, organizations can also monitor and record all of the privileged sessions involving changes to systems such as changes to configuration settings. All recordings are stored in the tamper-proof digital vault ensuring that users cannot delete or change activity records.

Additionally, organizations can ensure that no one can gain privileged access to a system unless the user provides an approved and validated change record. CyberArk's solution can perform validation against the organizations' Change Management system.

12.2.1 Controls against malware

With the CyberArk solution, organizations can implement controls to protect against malware. The CyberArk solution isolates, controls, and monitors privileged access and activities for critical systems such as UNIX and Windows-based systems, databases and virtual machines. The solution acts as a jump server and provides a single access control point, preventing malware from jumping to a target system. Isolation between an administrator's desktop and target systems reduces the risk of malware spreading to critical systems.

12.4.1 Event logging

The CyberArk solution generates a rich set of real-time data on all privileged account activity across an organization's IT environment. It provides centralized logging and recording of all privileged access to systems and stores all logs and recordings in a tamper-proof digital vault.

The solution provides detailed privileged session recordings for complete, command-level data or live session views on exactly what happens during a privileged session. DVR-style playback of sessions is provided for event analysis. Session recordings can be configured to include:

- Unique identity of the privileged user or application
- Dates and times
- Device or system identifiers
- Network addresses or protocols
- Specific actions taken such as system or resource access attempts, configuration changes, use of system utilities and applications, file access, or activation/de-activation of protection systems.

Organizations can also log all access to privileged account information in the vault, such as when passwords are retrieved, changed or used to execute privileged operations; as well as all privileged account management functions such as the addition of users or report generation.

Integrating with the world's leading solutions for event correlation and management, all log information and privileged session recordings are readily available to security operations teams to help identify and triage suspicious privileged activity, and stop attacks. The solution integrates with Security Information and Event Management (SIEM) and event log systems including HP ArcSight, Splunk, McAfee ESM, IBM/QRadar and RSA enVision for complete correlational analysis, including support for Syslog and XSL schema.

CyberArk also provides Privileged Threat Analytics, which uses proprietary algorithms to call attention to unusual activity that could indicate an in-progress attack. CyberArk Privileged Threat Analytics compares real-time privileged account activity to historical behavior in order to detect anomalies as they occur. These anomalies are then correlated to immediately determine whether they reveal malicious intent. By applying patent pending analytic technology to a rich set of privileged account behavior, the solution produces highly targeted and immediately actionable intelligence, allowing incident response teams to respond directly to the attack. In addition to a proprietary dashboard built into the system, data and alerts from CyberArk Privileged Threat Analytics can be integrated into an organization's existing SIEM system. The analytics on fine-grained privileged user behavior improves the effectiveness of the SIEM system by enabling targeted alerts on privileged account risks.

12.4.2 Protection of log information

With the CyberArk solution, all logs and session recordings for privileged account activity are protected by CyberArk's patented ICSA-certified Vaulting Technology®, which employs multiple built-in layers of security. CyberArk's tamper-proof digital vault uses AES 256 cryptographic storage and is FIPS 140-2 certified.

Access to logs and session recordings can be restricted to authorized users with a job-related need. Encrypted storage and strict access controls helps to ensure that unauthorized users or rogue administrators cannot edit or delete logs in order to erase evidence of malicious activity.

As well, access to the vault's logging and recording functions is strictly controlled and limited to authorized users. Any changes, such as altering the information being collected or activities being recorded, are monitored. This helps to protect logging and session recording from alteration or de-activation.

The CyberArk solution can be configured to retain logs and session recordings for a defined length of time. For archiving, the information can be sent to another system for back up via the syslog protocol.

12.4.3 Administrator and operator logs

As described in 12.4.1, the CyberArk solution generates a rich set of real-time data on all privileged account activity across an organization's IT environment. This includes all system administrator and system operator activities.

With centralized logging and recording of all privileged account activity, organizations can ensure adequate monitoring and review of system administrator and operator activities. The solution provides a single pane of glass management console for security operations teams and auditors to manage, access and review log information for all privileged users.

As described in 12.4.2, all event logs and recordings are fully protected and stored in a tamper-proof digital vault. See 12.4.1 and 12.4.2 for complete information on logging and the protection of log information.

12.4.4 Clock synchronization

CyberArk's Digital Vault™ can be synchronized to the enterprise time source ensuring that the vault's timestamps (such as those on audit records) correspond to the system time.

12.5.1 Installation of software on operational systems

To help control the installation of software on operational systems, the CyberArk solution enables organizations to ensure that only authorized users can gain the necessary level of privileged access. Access is restricted by controlling access to administrative passwords stored securely in the digital vault. "Dual Control" can specify that access to highly sensitive passwords requires confirmation by one or more authorized users, greatly limiting the ability to perform unauthorized updates to operational software. Organizations can log and monitor all updates to operational program libraries performed using privileged user credentials

For supplier access, the CyberArk solution helps ensure accountability for all third-parties provided with a privileged account and enables access to systems without revealing any privileged passwords. The organization can specify the time period for which the supplier is allowed access and disable access when not in use.

Further, the system can be configured so that all non-organizational users who remotely connect to the digital vault connect through a proxy so their session is isolated from the internal network, mitigating third-party risks. The CyberArk solution also monitors and records entire privileged account sessions by third-parties and integrates with Security Information and Event Management (SIEM) and event log systems for complete correlational analysis.

12.7.1 Information systems audit controls

The CyberArk solution enables auditing of all privileged access across an organization's IT environment. Organizations can automate controls for generating, protecting and reviewing the audit records; helping to minimize disruptions to business processes.

Organizations can also implement access controls to ensure that auditors can, for example, view audit records and reports but not view privileged credentials. All auditor activities can be monitored and logged including tracking when reports are run, which is useful for proving that auditors were supplied with specific reports with a timestamp.

13.1.1 Network controls

By managing privileged accounts with the CyberArk solution, organizations can ensure that systems on the network are properly authenticated and restrict connections to the network to authorized systems.

Instead of using hard-coded passwords which are typically in clear text within applications, the CyberArk solution effectively eliminates embedded application credentials. To perform designated tasks like connecting to a network resource, an application must first have authorized access to the privileged credential in the vault. To gain access to the credential, an application is authenticated using advanced authentication methods based on specific application characteristics including its server, operating system, and a crypto "fingerprint."

Only authorized applications with the appropriate characteristics can access systems on a network. Access to systems and connections to networks can be controlled by various restrictions such as date and time and the location from which the applications can request access.

13.1.2 Security of network services

See 9.1.2 for information on how the CyberArk solution helps organizations secure network services by restricting access to authorized users.

14.2.2 System change control procedures

For system change control procedures, the CyberArk solution helps organizations to ensure that only authorized users can gain access in order to submit changes. See 12.1.2. "Change Management" for more information on how the CyberArk solution supports system change control procedures.

14.2.6 Secure development environment

To ensure that only authorized users gain access to particular development environments, the CyberArk solution restricts access by controlling access to administrative passwords, which are stored securely in the digital vault and protected with strong encryption. The patented digital vault technology inherently supports separation of duties. The vault is divided into safes that are accessed by users based on their specific permissions and without knowledge of the existence of other safes.

15.1.1 Information security policy for supplier relationships

With the CyberArk solution, organizations can mitigate the risks associated with suppliers' privileged access to the organization's information assets. Access is restricted by controlling access to administrative passwords stored securely in the digital vault. Suppliers who remotely request access to the network gain access to the digital vault through a proxy so their session is encrypted and isolated from the internal network.

All supplier access to the network can be tracked to a unique user ID to ensure accountability, yet the solution enables access without revealing any privileged passwords. The organization can specify information access restrictions for different types of suppliers, including allowable access times; and can disable supplier access when not in use. The solution supports the implementation and enforcement of fine-grained least privilege policies. All privileged access and activities by suppliers can be monitored and recorded in real-time in order to intercept or de-activate the session if necessary.

15.1.3 Information and communication technology supply chain	As a trusted supplier of privileged account security products to organizations worldwide, CyberArk helps to address the risks associated with an organization’s information and communications technology supply chain. The CyberArk solution is enterprise-proven in large and mid-sized commercial and government organizations. The company fully supports its customers and enables complete life-cycle management of the product suites. Specifically: ▪ CyberArk’s products are highly acclaimed for their security engineering, including layered protection, security architecture, security training for developers and much more. ▪ The company provides configuration management, change tracking, and security updates. ▪ The products have all been internally and field-tested and used extensively by thousands of customers, providing the highest security assurance. ▪ To help ensure proper implementation and usage of the product suites, CyberArk provides full product documentation, comprehensive training for users and administrators and offers additional support through professional services. ▪ CyberArk’s products are validated by ICSA Labs and are FIPS 140-2 compliant.
16.1.7 Collection of evidence	As described in 12.4.1, the CyberArk solution generates a rich set of real-time data on all privileged account activity across an organization’s IT environment. This extensive information can serve as forensic evidence.
18.2.3 Technical compliance review	The CyberArk solution provides centralized policy management and reporting for all privileged access across an organization, enabling regular review for compliance to the security policy. Organizations can run automated compliance reports to ensure that access control policy is being enforced for all privileged accounts. Automatic discovery and provisioning of accounts ensures that even accounts hidden in services, scheduled tasks, application pools or local administrator groups are discovered and managed securely according to organizational policy.

Conclusion

By deploying the CyberArk Privileged Account Security Solution, organizations can implement the full range of controls within the ISO/IEC 27002:2013 standard related to securing privileged accounts. The solution's centralized management and reporting capabilities enable security reviewers, auditors, and ISO certification bodies to easily verify the management and control of privileged accounts, reducing the cost of assessments.

CyberArk's patented Digital Vault™ technology, military-grade encryption, robust reliability, and tamper-proof audit logs are designed to meet the highest security and compliance standards. Deploying CyberArk solutions not only helps organizations to comply with regulations but also to protect their most valuable information assets from advanced threats and reduce the risks of damaging and costly data breaches.

Appendix: The CyberArk Privileged Account Security Solution

Designed from the ground up with a focus on security, CyberArk has developed a powerful, modular technology platform that provides the industry's most comprehensive Privileged Account Security Solution. Each product can be managed independently or combined for a cohesive and complete solution for operating systems, databases, applications, hypervisors, network devices, security appliances and more. The solution is designed for on-premises, hybrid cloud and OT/SCADA environments.

The CyberArk Privileged Account Security Solution includes the following products:

Enterprise Password Vault® fully protects privileged passwords based on privileged account security policies and controls who can access which passwords when.

SSH Key Manager™ secures, rotates and controls access to SSH keys in accordance with policy to prevent unauthorized access to privileged accounts.

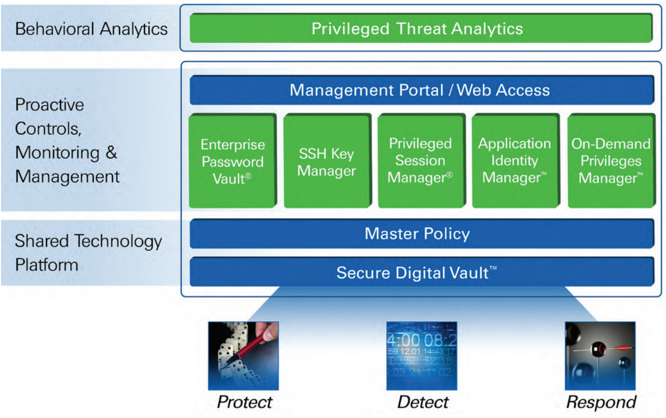
Privileged Session Manager® isolates, controls, and monitors privileged user access as well as activities for critical UNIX, Linux, and Windows-based systems, databases, and virtual machines.

Privileged Threat Analytics™ analyzes and alerts on previously undetectable anomalous privileged user behavior enabling incident response teams to disrupt and quickly respond to an attack.

Application Identity Manager™ eliminates hard-coded credentials, including passwords and encryption keys from applications, service accounts and scripts with no impact on application performance.

On-Demand Privileges Manager™ allows for control and continuous monitoring of the commands super-users run based on their role and task.

The CyberArk Privileged Account Security Solution is built on a common, Shared Technology Platform that delivers a single management interface, centralized policy creation and management, a discovery engine for provisioning new accounts, enterprise-class scalability and reliability, and the secure Digital Vault™. The individual products in the CyberArk Privileged Account Security Solution integrate with the shared platform, enabling organizations to centralize and streamline management.


Behavioral Analytics
Privileged Threat Analytics
Proactive Controls, Monitoring & Management
Management Portal / Web Access
Enterprise Password Vault®
SSH Key Manager
Privileged Session Manager®
Application Identity Manager™
On-Demand Privileges Manager™
Shared Technology Platform
Master Policy
Secure Digital Vault™
Protect
Detect
Respond

To help organizations get started with their privileged account security project, CyberArk offers a free assessment tool, CyberArk DNA™ (Discovery and Audit) that discovers and identifies privileged accounts throughout an enterprise. With a clear record of all service accounts, devices, and applications, CyberArk DNA helps organizations achieve an understanding of the size and magnitude of their privileged account security risk.