CyberQP

CyberQP ISO 27001:2022 Product Control Mappings

QGuard FRAMEWORK: ISO/IEC 27001:2022

Function	Control	Control Description	Requirement
Privilege Account Discovery & Remediation	5.17	Authentication Information	Ensuring the secure management of authentication credentials prevents unauthorized access to information systems, protecting sensitive data from being compromised.
	5.18	Access Rights	Controlling access rights ensures that access is granted based on the principle of least privilege, minimizing the risk of unauthorized access to sensitive information.
	8.02	Privileged Access Rights	Managing privileged access rights protects sensitive systems and data from unauthorized access, ensuring that only authorized individuals have elevated privileges.
Technician Passwordless Authentication, Tracking & Auditing	5.15	Access Control	Implementing access control measures ensures that access to information systems is properly managed and restricted, protecting sensitive data from unauthorized access.
	5.17	Authentication Information	Ensuring the secure management of authentication credentials prevents unauthorized access to information systems, protecting sensitive data from being compromised.
	8.05	Secure Authentication	Implementing secure authentication ensures that only authorized users can access information systems, protecting sensitive data from being compromised.
Privileged Account Just-in-Time Access	5.15	Access Control	Implementing access control measures ensures that access to information systems is properly managed and restricted, protecting sensitive data from unauthorized access.
	5.16	Identity management	Managing identities ensures that only authorized individuals have access to information systems, reducing the risk of unauthorized access and potential security breaches.
	8.15	Logging	Recording events through logging supports security monitoring and incident response, providing valuable information for investigating and mitigating security incidents.

CyberQP

QDesk FRAMEWORK: ISO/IEC 27001:2022

Function	Control	Control Description	Requirement
Endpoint Privilege Management	5.18	Access Rights	Controlling access rights ensures that access is granted based on the principle of least privilege, minimizing the risk of unauthorized access to sensitive information.
	8.02	Privileged Access Rights	Managing privileged access rights protects sensitive systems and data from unauthorized access, ensuring that only authorized individuals have elevated privileges.
Identity Verification	5.18	Access Rights	Controlling access rights ensures that access is granted based on the principle of least privilege, minimizing the risk of unauthorized access to sensitive information.
	8.32	Change Management	Controlling changes to information systems prevents unauthorized modifications and potential security risks, maintaining the integrity and security of organizational data
Self-Service Password Reset (SSPR)	5.16	Identity management	Managing identities ensures that only authorized individuals have access to information systems, reducing the risk of unauthorized access and potential security breaches.
	5.17	Authentication Information	Ensuring the secure management of authentication credentials prevents unauthorized access to information systems, protecting sensitive data from being compromised.
	8.02	Privileged Access Rights	Managing privileged access rights protects sensitive systems and data from unauthorized access, ensuring that only authorized individuals have elevated privileges.
	8.03	Information Access restriction	Restricting information access based on need-to-know principles limits exposure to sensitive information, protecting it from unauthorized access and potential security breaches.
	8.15	Logging	Recording events through logging supports security monitoring and incident response, providing valuable information for investigating and mitigating security incidents.
Essential Account Management	5.16	Identity management	Managing identities ensures that only authorized individuals have access to information systems, reducing the risk of unauthorized access and potential security breaches.
	5.18	Access Control	Controlling access rights ensures that access is granted based on the principle of least privilege, minimizing the risk of unauthorized access to sensitive information.
	8.15	Logging	Recording events through logging supports security monitoring and incident response, providing valuable information for investigating and mitigating security incidents.

CyberQP redefines Zero Trust Access Management with leading-edge Privileged Access Management (PAM) and End-User Access Management (EUAM) solutions. Our platform enables secure elevated access for both IT Professionals and end-users, along with robust self-serve and identity verification capabilities. Backed by SOC 2 Type 2 certification, we empower IT professionals to reduce or eliminate risks stemming from social engineering attacks, standing privilege, and over-privileged accounts, enforce compliance, and enhance operational efficiency. Our mission is simple: "Empowering Access, Redefining Privilege" for security-focused IT professionals around the globe. Learn more **https://www.bluechipit.com.au/cyberqp/**