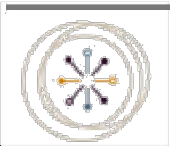

Privileged Access and Administration

Lifecycle management of credentials with elevated access required to administer critical systems infrastructure should be meticulously managed. From policy formation, to entitlement definition through credential assignment, there should be adequate controls to demonstrate approval and necessity of privileged access. The relationship of processes and technologies enabled to support privileged access administration should be taken into consideration based on the infrastructure footprint and regulatory needs of an organization. Controlling access to specific devices, service accounts, and administrative consoles across various development, staging and production environments has become a daunting task. As regulations continue to evolve it will be paramount for IAM programs to enable efficiencies surrounding the assignment, monitoring and auditing of individual users or devices to situational-appropriate privileged credential usage.

Governance and administration of users or devices with privileged access should be thoughtfully aligned to achieve sustainability and regulatory compliance

Core Capabilities

- Privileged Access Administration
- Password Vault
- Session Recording
- Jump Server Access
- Privileged Access Certification Processes

Regulatory Considerations

- PCI DSS Requirement 6: Develop and maintain secure systems and applications
- PCI DSS Requirement 7: Restrict access to cardholder data by business need to know
- PCI DSS Requirement 8: Assign a unique ID to each person with computer access
- PCI DSS Requirement 10: Track and monitor all access to network resources and cardholder data

7701 France Ave, Suite 400, Edina, MN 55435 ph. 651.259.1001