Key Gaps Identified Through the HITRUST Assessment

Policy & Procedure

Security policies exist but are outdated, inconsistently applied, or lack supporting evidence.

Risk Assessment Practices

These are often infrequent, leaving emerging threats insufficiently addressed.

Vulnerability Management

Delays in patching and remediation expose critical systems to preventable security risks.

Third-Party Risk Oversight

Vendors may not undergo adequate due diligence or continuous security monitoring.

Incident Response Preparedness

Response plans are not regularly tested, resulting in unclear roles during security incidents.

Access Management Controls

Excessive privileges and inadequate access reviews increase the risk of unauthorized access.

Audit Logging & Monitoring

Limited visibility into security events delay threat detection and response efforts.

Asset Inventory Management

Incomplete asset inventories make it difficult to protect and monitor critical resources.

Security Awareness & Training

Employees may lack role-specific training, increasing the likelihood of human error.

Data Protection Controls

Weak data classification, encryption, and key management practices compromise sensitive information.

www.ampcuscyber.com | letsconnect@ampcuscyber.com