TEVORA

One Spectrum Pointe Drive, Suite 200
Lake Forest, California 92630
t: 949.250.3290 | **e:** info@tevora.com

SECURITY CONTROLS ASSESSMENT

Tevora provides business process optimization for information security. We help organizations understand their current information security control risks, and develop a plan for improving those risks over time. Tevora partners with many solution providers to provide vetted and objective security solution recommendations for organizations of all sizes, across all industries.

GAIN SECURITY CONTROLS INSIGHT

A comprehensive view into the effectiveness and maturity of existing security controls is an essential part of overall organizational security.

Tevora's Security Controls Assessment is designed to thoroughly assess your organization's overall processes and security solution implementation. This assessment is conducted with IT administrators, information security professionals, systems administrators, database administrators, network engineers and other key personnel that are responsible for building and maintaining the organization's security controls. Tevora provides contextual control design guidance based on the information security risks uncovered during the assessment.

Tevora's assessment serves as a basis for developing a comprehensive long-term security program. Assessments are based on either the CIS Critical Security Controls or the NIST Cybersecurity Framework. Control maturity is measured using the COBIT 5 maturity model. Tevora also deploys a number of tools to provide empirical information about cloud security usage, privileged account usage, network device and firewall configuration and advanced malware detection in addition to the CIS or NIST control review.

1 ASSESS

- Assess the current infrastructure, processes and controls
- Score the maturity of processes and identify areas of improvement
- Document major deficiencies and exceptions based on established frameworks
- Deploy assessment tools that look for existing indicators of attack and compromise
- Analyze network architecture and your organization's ability to detect and respond to an attack

2 STRATEGIZE

- Provide recommended security program improvements based on assessment findings
- Develop a prioritized plan based on quickest time-to-value for risk mitigation within information security
- Integrate current solutions, personnel and expertise into the improvement plan

3 ROADMAP

- Develop a comprehensive report providing all findings and the current state of all security controls
- Define recommended to-be state for all controls
- Provide financial analysis and guidance for future expenses required to meet to-be state objectives
- High-level findings presentation providing an overview of the findings and recommendations report