AURORA

Cyber Security Risk Assessment

# Cyber Security Risk Assessment

*Our solution uses quantitative and qualitative methods to define the current and future state of your security environment in a complete internal and external Cyber Security Risk Assessment. We determine how your organization maps to best practices, along with the steps needed to get to the next level of security, and maintain a robust security environment as change occurs. A Cyber Security Risk Assessment identifies deficiencies and correlates them to practical solutions.*

## How the process works:

- Define a scope of each process and function being reviewed
- Gather all current documentation (policies, procedures, configuration standards, best practices used)
- Conduct internal and external vulnerability scanning
- Conduct penetration testing against your network systems
- Interview individuals and document how the processes of the business functions
- Compare security practices to best practices
- Prioritize the gaps and create a remediation plan
- Produce a qualitative risk report

## Key value propositions include:

- Understand gaps in regulatory compliance requirements
- Understand weaknesses in existing policies, procedures and standards
- Determine weaknesses in access controls, user provisioning, configuration management, vulnerability management processes, and incident handling processes
- Review of network, operating system, application and end-point security measures
- Development of key remediation recommendations

## BUSINESS VALUE

- Cost-effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge transfer

## FEATURES & BENEFITS

- Complete overall network security gap analysis
- Consistent and repeatable testing
- Continuously expanding vulnerability tests
- Comply with industry-driven regulatory requirement

## Cyber Security Risk Assessment Steps

| Steps | Professional Level | Enterprise Level |
|---|---|---|
| Automated Security Scanning: Commercial scanning tools used to identify potential vulnerabilities. | 🛡 | 🛡 |
| Report Development and Interpretation: Analyze results and remove false positives. | 🛡 | 🛡 |
| Network Architecture Review: Review network security design and identify weaknesses. | 🛡 | 🛡 |
| Manual Exploit Testing: Perform manual in-depth testing techniques to validate weaknesses in sample list of devices. | 🛡 | 🛡 |
| Security Policy Review: Review up to 5 security policies for gaps in procedures. | 🛡 | 🛡 |
| Remediation Validation: Perform mini-assessment after 6 months to validate remediation steps have been implemented. | | 🛡 |
| Policy Creation: Create or modify up to 5 policies to meet gaps in the security procedures. | | 🛡 |
| Compliance Needs Assessment: Review business operations and determine regulatory requirement applicability. | | 🛡 |

## Ready To Get Started?

**Contact us at 888-282-0696 or sales@aurorait.com to learn how Aurora Security Services can help you accomplish your specific business and IT security goals. Explore further by visiting our website at: www.aurorait.com**