TANGIBLE SECURITY

SECURITY PROGRAM ASSESSMENT & ROADMAP

AM I MATURE?

Gauge Your Cyber Security Program to Improve Your Security Posture and Reduce Business Risks

Tangible Security's **Security Program Assessment and Roadmap Development** measures the maturity of your security program and delivers actionable recommendations that will improve your security posture, reduce risk, and increase your cyber resilience.

Tangible uses standards such as NIST, ISO, COBIT or other formats as a starting framework, coupled with our expertise to understand your security program's current state and gaps to determine its capability maturity level. Tangible will work with you to examine the quality and effectiveness of your program, identify and understand weaknesses and vulnerabilities, and evaluate your readiness to defend and respond to today's cyber threats.

Additionally, Tangible may incorporate a cyber resilience review (CRR) as part of the assessment. The CRR is based on DHS CERT standards, and measures incident response management capability.

Tangible can also perform a technical configuration assessment, to ensure that a sample of the security devices are configured correctly and best able to provide protection when needed.

01 IDENTIFY	02 PROTECT	03 DEFEND	04 RESPOND	05 RECOVER

TANGIBLE RESULTS

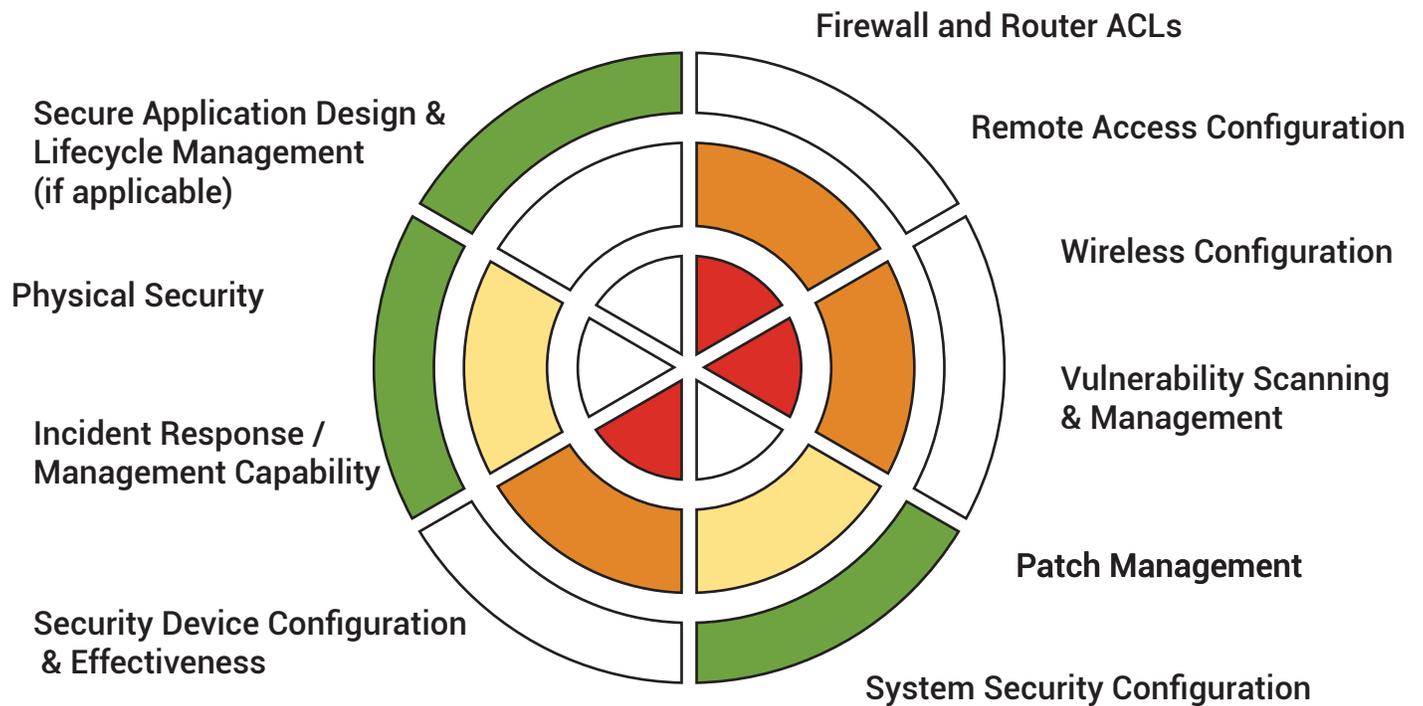After the Security Program Assessment, you will:

- Understand how you are managing cyber risks

- Identify security gaps, ineffective operational processes and poor technology security controls

- Be able to define a security strategy and roadmap to address current and emerging threats

- Maximize your return on investment in cybersecurity

SECURITY PROGRAM AREAS COVERED

- Security Program Strategy and Architecture Governance

- Gap Assessment (based on ISO 27001, NIST, HIPAA, GDPR, PCI DSS, COBIT, or other standard)

- Cyber Resilience Review (CRR) based on DHS CERT standards for Incident Response

- Policies and processes including:
  - Overall Security
  - Access Control
  - Data Protection
  - Vulnerability Management
  - Incident Management
  - Secure System Configuration
  - Configuration Control
  - Wireless Use
  - Security Reporting and Metrics
  - Security Awareness Training

TECHNICAL CAPABILITIES REVIEWED

In addition to policies, the Security Program Assessment reviews the technical capabilities of your security posture, identifying capability gaps or configuration errors, and suggest ways and priorities to improve.

- Firewall and Router ACLs
- Remote Access Configuration
- Wireless Configuration
- Vulnerability Scanning & Management
- Patch Management
- System Security Configuration
- Secure Application Design & Lifecycle Management (if applicable)
- Physical Security
- Incident Response / Management Capability
- Security Device Configuration & Effectiveness

ROADMAP DEVELOPMENT

Tangible Security will build on the findings during the Security Program Assessment and create a Security Roadmap, taking into consideration:

- Findings from recent Cyber Security Assessments
- Findings from the Security Program Assessment
- Your specific business goals and budget
- Your Information Security capability and staffing level
- Your Regulatory and Industry Compliance Requirements

A security "Current State" is established during the Security Program Assessment. A custom Security "Target State" will be established during the Security Roadmap Project that takes into consideration Test Company's specific industry and compliance requirements.

The Security Roadmap typically outlines a three year strategic and tactical plan with recommendations on sequencing and prioritization for improving the effectiveness of your Security program's Maturity Level over time, and will also provide preliminary budget information for planning purposes.

Email: info@TangibleSecurity.com
Phone: 757-525-1863
www.tangiblesecurity.com

Tangible Security
PO Box 508
Dunn Loring, VA 22027