CYBERSECURITY AND COMPLIANCE ASSESSMENT

Armor's cybersecurity and compliance assessment delivers a baseline assessment for your organization's overall cybersecurity and compliance posture. The review provides a picture of your organization's existing approach for "people, process, and technology," a recommendation on what is needed to combat threats facing your organization, and, finally, a path to reaching your desired state of maturity.

MANAGE RISK TO PROTECT YOUR BRAND

Hackers are constantly evolving their tactics and expanding their targets to gain unauthorized access to data. At the same time, nearly every business faces the challenge of achieving and maintaining compliance with required standards. Knowing where your organization stands, for both security and compliance, is a critical first step in meeting your goals.

KEY LEVELS OF ARMOR'S MATURITY MODEL FOR SECURITY AND COMPLIANCE

Business value increases and risk decreases with increased security and compliance maturity.

1	2	3	4	5
INITIAL 1.0	DEVELOPING 2.0	DEFINED 3.0	MANAGED 4.0	OPTIMIZED 5.0

|

ARMOR

KEY SERVICE FEATURES

DISCOVERY
We map your existing environments.

ASSESSMENT
Next, we assess your environments as they relate to applicable compliance standards. Analysis includes identification of known vulnerabilities, policy violations, and more.

REPORTING
Our team of experts compiles a baseline for your compliance and security maturity along with a prioritized list of recommendations. This includes suggested remediation.

REALIZATION
Finally, we enable continuous monitoring and notifications within our security platform to effectively manage cybersecurity and compliance requirements going forward.
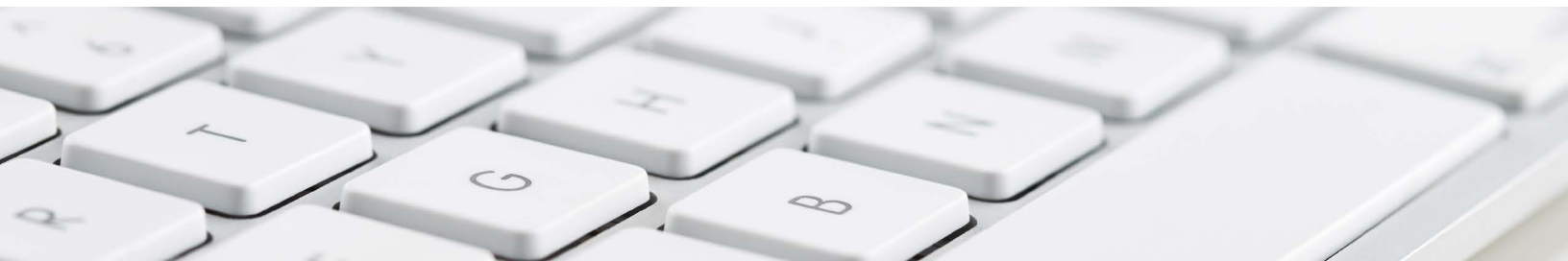
KEY BENEFITS

IDENTIFIES WEAK POINTS
Proactively discovers gaps that introduce risk.

PRIORITIZES IMPROVEMENTS
Offers detailed recommendations on how to improve your posture.

CUSTOMIZES RECOMMENDATIONS
Suggests enhanced compliance and security practices that help protect your organization from threats.

ARMOR