Solution Brief

Governance, Risk and Compliance (GRC) Assessment Services

Insight cybersecurity

GRC requirements

Organizations are looking for ways to operate more securely and are bound by regulatory requirements specific to their industry and operations. Failure to use best practices to secure critical assets and data may lead to inefficient operations, loss of consumer confidence and risk of regulatory fines. Insight understands this challenge facing clients and offers a comprehensive list of assessment, testing and auditing services.

Challenges with security compliance

Regulation awareness

It's difficult to maintain knowledge of the complex and changing regulatory, industry and compliance requirements.

Security program maintenance

Managing appropriate levels of security and end-user functionality is either ineffectively administered or processes are not well established.

Resource challenges

Lack of resources could lead to increased exposure from either improper security control configurations or unknown third-party risks.

We can help you go beyond just identifying gaps.

Insight's assessment solutions provide an analysis of security gaps as well as recommendations aligned to remediate those gaps. Insight can also help you take your recommendations further by:

- Establishing a roadmap to improve security posture, which may include items such as resource augmentation, threat visibility solutions and improvements to security configurations
- Developing or refining security policies to increase consistency across access controls, network security, asset management and more
- Providing remediation services aligned with enhanced security policies and procedures such as implementing least privilege access or network segmentation

Benefits

Best practices
Reduce risk by following cybersecurity best practices.

Meeting requirements
Remain compliant with regulatory requirements.

Cost savings
Reduce costs from minimizing exposure to risks and avoiding fines and penalties.

Related services

Vulnerability Management Program Review

Penetration Testing Services

Identity and Access Management Assessment

Zero Trust Maturity Assessment

Managed Security Services

Delivery approach

Insight offers readiness assessments, audits and security framework assessments based on current business requirements.

Stakeholder interviews

Analysis and data gathering

Draft deliverable

Final deliverable

*Optional roadmap

Framework assessments	
3rd Party Risk Assessments	Security posture and practices of external vendors, suppliers or partners, especially those that have access to an organization's data or systems
Additional assessments available	Specialty frameworks, directives or security needs (e.g., Industrial Controls Systems (ICS))
Center for Internet Security (CIS) Critical Controls Assessment	Identifies security controls implemented to protect against modern threats to systems and software
Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E)	Affordable Care Act (ACA) entities, contracts or subcontractors' security practices based on the set of ACA privacy and security standards
Cybersecurity Maturity Model Certification (CMMC) Assessment	Federal contractors' and subcontractors' security solutions, which protect shared federal contract information and CUI
International Organization for Standardization (ISO) 27001/27002	Policies, procedures and security controls for Information Security Management Systems (ISMS)
National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) 2.0	Policies, procedures and processes based on the core framework functions: Govern, Identify, Protect, Detect, Respond and Recover
NIST 800-171 R2	Protecting Controlled Unclassified Information (CUI) in nonfederal systems and organizations
NIST 800-53	Strength of security and privacy controls for federal information systems
Payment Card Industry Data Security Standard (PCI DSS)	Audits or assesses policies and controls implemented for storing, processing or transmitting credit card data
Privacy Assessments	Policies, procedures and processes that control personal data and ensure personal data is processed lawfully, fairly and transparently
Transportation Security Administration (TSA) Security Directive	Cybersecurity program policies, testing, reporting and documentation assessed against the Security Directive pipeline

Driving innovation with digital transformation

At Insight, we help clients enable innovation with an approach that spans people, processes and technologies. We believe the best path to digital transformation is integrative, responsive and proactively aligned to industry demands. Our client-focused approach delivers best-fit solutions across a scope of services, including the modern workplace, modern applications, modern infrastructures, the intelligent edge, cybersecurity, and data and AI.

Learn more at insight.com.

Insight

insight.com