RSI | Datasheet

The GRCS Approach

One of the most common—and effective—ways to manage your cyberdefense infrastructure is bundling together the areas of Governance, Risk Management, and Compliance (GRC) under one program. While this strategy has served countless organizations well over the past few decades, an even more impactful approach is adding Security to the mix for a GRCS program.

There are four essential components to a robust, flexible GRCS program:

Data Governance Program

Governance provides fundamental definitions of what sensitive data needs to be protected, why, and how—along with where it's located and who is most responsible for protecting it.

Risk Management Program

Risk management comprises practices for detecting, identifying, analyzing, preventing, and responding to vulnerabilities and threats, mitigating potential impacts on cyber assets.

Compliance Management Program

Compliance management involves practices of implementing and then assessing controls from regulatory frameworks to protect special classes of data and maintain certification.

Information Security Program

Information security includes selecting, installing, and optimizing appropriate controls, then regularly monitoring effectiveness with assessments, employee training, and more.

Taken together, these elements feed off of and synergize with each other. Effective risk management works hand-in-hand with information security; performing both makes for streamlined compliance. And strong governance ensures smooth, efficient operations.

Benefits of a GRCS Approach to Cyberdefense

By including Information Security alongside Governance, Risk Management, and Compliance, organizations ensure that all elements of cyberdefense work in concert. This maximizes the effectiveness of each individual component, such that the combined effect is greater than the sum of its parts. It also reduces inefficiencies, like costly overlapping controls, to maximze ROI.

RSI Security's GRCS Services

RSI Security offers a suite of GRCS services, many of which may be utilized individually or as part of a cohesive GRCS program. In particular, our services under each component include:

1 Data Governance Services

- Data Health Check
- Data Classification and Categorization
- Data Discovery
- Data Access Control Review
- Data Security Implementation
- Technical Writing

2 Risk Management Services

- Risk Assessments
- Risk Registry
- Impact Analysis
- Continuity Plan
- Disaster Recovery
- Incident Response
- Risk Management Implementation
- 3rd Party Risk Assessment

4 Compliance Management Services

- Coverage for PCI DSS, HITRUST, CMMC, HIPAA,
- SOC 2, and more
- Advisory and Assessment
- Remediation Plans
- Assessment and Certification

4 Information Security Services

- Framework-based Assessments
- Identity, Access, and Authentication
- Firewall, IPS, EDR, NDR, etc.
- Staff Awareness and Training
- Managed Security

Rethink Governance, Risk Management, Compliance, and Security

Too often, organizations take a defensive and reactive approach to cybersecurity. To combat the growing threats of cybercrime and advanced persistent threats, a more multi-faceted approach is critical. Keeping your data secure means making sure that Governance, Risk Management, Compliance, and Information Security practices are working together rather than separately.

GRCS empowers proactive, preventive security. It stops threats from emerging and facilitates swift, full remediation when a cyberattack or other event does occur—especially when working with us.

About RSI Security

RSI Security provides GRCS and other cybersecurity services to organizations of all sizes and across all industries. Our expert leadership leverages decades of experience to streamline and optimize security controls and overall management so that organizations like yours can focus their resources on direct business functions. Partner with RSI Security to rethink your cyberdefenses.

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com