Governance, Risk and Compliance Services

IDC's *Governance, Risk and Compliance Services* program provides C-level executives and security service providers with insights into how to effectively measure and quantify cybersecurity risk and compliance for their respective impact to the business, whether service or software. Tying this all together with a governance services and software view ensures that every component of these programs is operating optimally and continuously. A derivative of enhanced risk and compliance is trust.

Holistic governance, risk, and compliance (GRC) services and software solutions enable organizations to manage risk across a broad range of enterprise risk domains and/or enable these risk domains to be managed by qualified cybersecurity services providers. Cybersecurity GRC is a subsector of holistic GRC and focuses on all aspects of cybersecurity risk and compliance across the enterprise. Cybersecurity GRC consists of numerous capabilities and activities that are required to identify, catalog, track, analyze, monitor, and report risks and compliance deficiencies required to enhance performance and be compliant with laws, regulations, industry standards, and organization policies. This program will aid cybersecurity firms to engage organizations on cybergovernance, risk, and compliance; privacy and trust; and market/position cybersecurity service offerings strategically and align to business objectives and outcomes.

MARKETS AND SUBJECTS ANALYZED

The cybersecurity software and services segment will cover:

- GRC services and software advisory, strategy, design, implementation, life-cycle management, and trends
- Risk, compliance, and privacy assessments; modeling; quantification; frameworks; maturity; and mitigation
- Implementation, knowledge transfer, and training and staff augmentation
- Cybersecurity insurance
- GRC program managed services

The specific areas of coverage include:

- Third-party and supply chain risk management services
- Continuous compliance, integrated risk management, and insider risk
- GRC automation, orchestration, and artificial intelligence

CORE RESEARCH

- Comprehensive GRC services and software including consulting, integration, professional services, security education services, and software and managed services
- GRC vendor profiles and benchmarks GRC survey results
- IDC PlanScapes, TechScapes, MarketScapes, and Taxonomy

- IDC Market Forecasts and Market Shares and IDC Market Analysis Perspective
- Continuous compliance and integrated risk management
- GRC services and software enablers

In addition to the insight provided in this service, IDC may conduct research on specific topics or emerging market segments via research offerings that require additional IDC funding and client investment. To learn more about the analysts and published research, please visit: Governance, Risk and Compliance Services.

KEY QUESTIONS ANSWERED

1. What are the key cyber-risk objectives to demonstrate to the board? (Hypothetical answers include due diligence, ownership, effective management, leader and organizational talent, and cyberculture.)
2. What are the appropriate cybersecurity frameworks to determine risks and ongoing compliance? How do organizations measure against these frameworks?
3. What is the overall cybersecurity risk appetite, and how should proper budgeting be established to address the appetite?
4. How do cybersecurity programs and capabilities align to industry standards and peer organizations?
5. What are the necessary third-party and supply chain cyber-risk management considerations?
6. What is the security posture of an organization at any point in time?
7. Do organizations have governance, risk, compliance, and privacy programs in place? How are these programs measured, and are they managed in-house or outsourced?
8. How are cyberattacks affecting the cost of cyberinsurance and the types of cyberinsurance products?

COMPANIES ANALYZED

This service reviews the strategies, market positioning, and future direction of several providers in the governance, risk, compliance, and privacy service and software market, including but not limited to:

Accenture, AT&T, BT, Cisco, Coalfire, D&B, Deloitte, Diligent, EY, HCLTech, HP, IBM, Infosys, KPMG, Kyndryl, Mandiant, NAVEX, Optiv, Palo Alto, PwC, Safe Security, ServiceNow, Tanium, Tata Consultancy Services (TCS), Trustwave, Vanta, and Verizon.