Governance, Risk and Compliance Services

AN IDC CONTINUOUS INTELLIGENCE SERVICE

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 and their impact to the business. Tying this altogether with a governance view ensures that every component of these programs are operating optimally and continuously. A derivative of enhanced risk is trust.

Through survey research and direct dialogue with the C-suite, this program will help cybersecurity services firms identify opportunities to engage with organizations around the topic of cyber governance, risk, and compliance (GRC), privacy, and trust and to help market/position their cybersecurity service offerings strategically within organizations, with a stronger alignment to business objectives and outcomes.

Markets and Subjects Analyzed

The professional security services segment will cover:

- GRC and privacy advisory and assessment services including the alignment of cybersecurity and business risk, stakeholder alignment, risk modeling, and trends
- GRC and privacy program strategy, design, and implementation services throughout the life cycle
- Cybersecurity frameworks, methodologies, and platforms
- Cyberinsurance
- Qualitative versus quantitative versus maturity views

The managed security services segment will cover:

- Management, execution, and monitoring of the GRC and privacy program on behalf of the client
- Risk treatment and mitigation strategies
- Third-party and supply chain risk management services

Core Research

- Cybersecurity Risk Survey Results
- IDC PlanScape
- IDC MarketScape
- IDC Market Analysis Perspective
- IDC TechScape
- Market Forecast
- Taxonomy

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 market, including but not limited to:

Accenture, AT&T, BT, Cisco, Coalfire, Deloitte, Diligent, E&Y, HP, IBM, Infosys, KPMG, Kroll, Mandiant, NTT, Optiv, Palo Alto, PWC, Safe Security, Secure Digital Solutions (TrustMAPP), Tata Consultancy Services (TCS), Trustwave, and Verizon.