



Governance, Risk, & Compliance Services

Expert-led governance, proactive risk management, and seamless compliance—so your business stays secure and audit-ready.

The Challenge

Compliance with regulatory requirements is growing ever more complex, and the repercussions of non-compliance are at an all-time high. Organizations face the daunting task of maneuvering through a tangled landscape of security frameworks, industry standards, and government regulations, all while balancing business risks and protecting sensitive information. Are you truly confident that your policies, processes, and controls can endure a regulatory audit? Do you possess complete visibility into your organization's cybersecurity vulnerabilities? It's crucial to assess your readiness now—don't leave your compliance to chance.

Our Solution

At CyberClan, we empower businesses to take control of their Governance, Risk, and Compliance (GRC) strategy through expert consulting services aimed at mitigating threats, ensuring compliance, and building resilience. Our team of cybersecurity professionals possesses deep industry expertise that helps streamline risk management, achieve regulatory compliance, and strengthen security posture—allowing you to focus on what matters most: growing your business.

Governance: A well-structured governance framework is essential for maintaining a resilient cybersecurity program. Our team collaborates with organizations to develop and implement security policies, procedures, and control frameworks that align with industry best practices and regulatory requirements.

Key deliverables include:

- **Security Policy Development:** Creation of comprehensive policies covering access control, incident response, data protection, and more.
- **Roles and Responsibilities Definition:** Establishing accountability across executive leadership, IT teams, and security personnel.
- **Security Oversight and Reporting Mechanisms:** Conduct regular security assessments, provide board-level reporting, and utilize compliance dashboards to ensure visibility into the organization's security posture.

Risk Management: Cyber threats are constantly evolving, requiring organizations to take a proactive approach to risk management. Our services help businesses identify vulnerabilities, assess threats, and implement mitigation strategies to minimize exposure.

Key components include:

- **Threat Assessments and Risk Analysis:** Conducting in-depth assessments to evaluate cybersecurity risks, attack vectors, and potential business impacts.

- **Customized Risk Management Plans:** Developing tailored risk mitigation strategies, including incident response playbooks and crisis management protocols.
- **Managed Security Awareness Training Program:** Our program provides a tailored approach to security education, developed by experienced professionals. This 12-month program empowers employees, achieving phishing rates as low as 1%, and fosters a security-conscious culture.

Compliance: Navigating complex compliance requirements can be challenging, especially as regulations continue to evolve. We ensure organizations meet industry standards such as NIST-CSF, CIS Top 18, CMMC Level 1 readiness, HIPAA, and ISO by providing the following:

- **Compliance Gap Assessments:** Evaluating current security measures against regulatory mandates to identify and address deficiencies.
- **Policy and Procedure Development:** Crafting documentation and security policies tailored to compliance requirements.
- **Audit Readiness and Reporting:** Conduct internal readiness and third-party assessments and prepare detailed reports to demonstrate regulatory adherence.

Key Benefits

- Identify vulnerabilities and establish a baseline to standardize result analysis.
- Prioritize recommendations to close security gaps and maintain a strong cybersecurity posture.
- Educate and train the entire organization to enhance the human firewall.
- Evaluate and iterate existing frameworks to strengthen your security posture while keeping current with threat intelligence—at a fraction of the cost of in-house resources.