Public Sector Cybersecurity Governance and Legal Compliance Training Course

Ref: #SM7066

Course Introduction / Overview:

Cybersecurity is a critical function for government entities, where protecting citizen data, public infrastructure, and national security is of the utmost importance. This training course provides a detailed look at the principles of cybersecurity governance and legal compliance specifically for the public sector. We will cover the key frameworks, policies, and regulations that govern information security in government, including NIST and other internationally recognized standards. Participants will learn how to develop a robust cybersecurity governance structure, conduct risk assessments, and make sure their agency's practices are in full compliance with legal requirements. We will explore academic work by authors like Ryan Ellis and Vivek Mohan, whose book Rewired: Cybersecurity Governance provides a strategic perspective on the topic. The curriculum is designed to equip professionals with the knowledge to build a secure, resilient, and legally compliant cybersecurity program. The BIG BEN Training Center is committed to providing a program that helps government entities navigate the complex landscape of cyber threats and regulations. By the end of this program, participants will be equipped with the knowledge to protect their organization's assets and public trust.

Target Audience / This training course is suitable for:

- Chief Information Security Officers (CISOs).
- IT and cybersecurity managers in government agencies.
- Compliance and risk management officers.
- Legal professionals in the public sector.
- Senior administrators and policymakers.
- Auditors and internal control specialists.
- Technology and systems architects.

Target Sectors and Industries:

- Government and public administration.
- Defense and national security.
- Public utilities and critical infrastructure.
- Healthcare and social services.
- Financial regulatory bodies.
- Education and research institutions.
- Government agencies and their equivalents.

Target Organizations Departments:

- Information Technology (IT).
- Cybersecurity and Information Assurance.
- Legal and Compliance.
- Risk Management.
- Internal Audit.
- Human Resources.
- Operations.

Course Offerings:

By the end of this course, the participants will have able to:

- Establish a cybersecurity governance framework for a government entity.
- Identify and comply with relevant cybersecurity laws and regulations.
- Develop and implement policies for data protection and privacy.
- Conduct a cybersecurity risk assessment for public sector systems.
- Understand the roles and responsibilities of key stakeholders in governance.
- Use frameworks like NIST to improve cybersecurity posture.
- Implement strategies for secure data management and access control.
- Create an effective and legally sound incident response plan.

Course Methodology:

This training course uses a blend of instructional and hands-on methods to make sure the content is engaging and practical for public sector professionals. The program begins with instructor-led sessions that provide a clear understanding of the core principles of cybersecurity governance and compliance. A key component of our approach is the use of real-world case studies and examples of legal compliance issues in government. Participants will analyze these scenarios to understand the legal and reputational risks involved, helping them to apply the principles in a real-world context. We also use interactive workshops and group exercises where participants work together to develop a governance framework for a mock government agency. This collaborative learning model encourages teamwork and allows participants to practice their decision-making skills. Instructors at BIG BEN Training Center are experienced professionals who provide continuous feedback and guidance throughout the course. Our goal is to prepare professionals to face the unique legal and compliance challenges of the public sector. By focusing on practical, actionable knowledge, we are making sure that every participant leaves the course ready to create a more secure and legally compliant organization.

Course Agenda (Course Units):

Unit One: The Foundation of Cybersecurity Governance.

- Understanding the importance of governance in the public sector.
- Key cybersecurity governance frameworks and models.
- The role of leadership in establishing a security-conscious culture.
- Defining roles and responsibilities for cybersecurity.
- The lifecycle of cybersecurity governance.

Unit Two: Legal and Regulatory Compliance.

- An overview of key cybersecurity laws and regulations.
- The importance of data privacy laws.
- Compliance requirements for government entities.
- Best practices for legal reporting and documentation.
- The legal implications of data breach.

Unit Three: Risk Management and Policy Development.

- Conducting a cybersecurity risk assessment.
- Developing and implementing security policies.
- Managing third-party and supply chain risks.
- The use of security metrics and key performance indicators.
- Continuous monitoring and control management.

Unit Four: Securing Data and Systems.

- Data classification and protection.
- The principles of access control and identity management.
- Securing cloud services in the public sector.
- Secure configuration and vulnerability management.
- Auditing and internal controls.

Unit Five: Incident Response and Business Continuity.

- Creating a legally compliant incident response plan.
- The importance of a communication strategy during a crisis.
- Post-incident review and learning.
- Integrating business continuity into cybersecurity.
- The role of governance in long-term resilience.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

In an environment where technology is evolving faster than legislation, how can government entities create a sustainable and agile cybersecurity governance framework that remains effective in the face of new and unforeseen legal and regulatory challenges?

What unique qualities does this course offer compared to other courses?

This training course is unique because it is designed specifically for the public sector, addressing the unique challenges of cybersecurity governance and legal compliance that government entities face. While many cybersecurity courses focus on the technical aspects, our program places a strong emphasis on the governance, policy, and legal frameworks that are critical for public organizations. The curriculum goes beyond generic best practices and provides a practical roadmap for complying with specific government-related regulations. It also uses a hands-on, scenario-based methodology, allowing participants to work through real-world legal and compliance dilemmas. We focus on how to build a security culture and gain buy-in from all levels of an organization. The course also bridges the gap between the technical teams and legal departments, helping to create a more cohesive and effective security posture. BIG BEN Training Center is committed to providing a program that gives government professionals the knowledge and skills they need to protect public assets and maintain public trust.