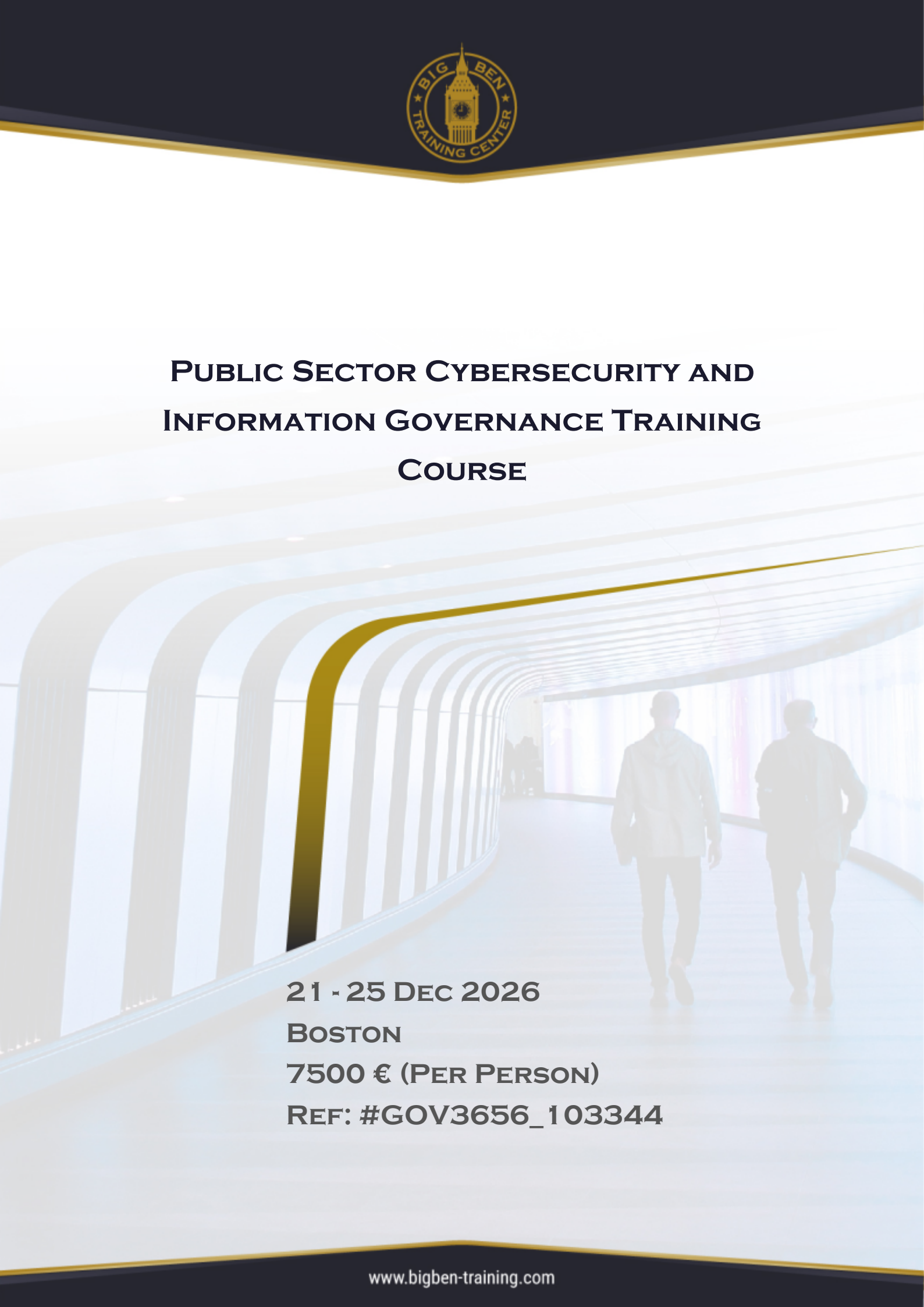
Public Sector Cybersecurity and Information Governance Training Course



21 - 25 Dec 2026

Boston

7500 € (Per Person)

Ref: #GOV3656_103344

Course Introduction / Overview:

This comprehensive course provides an in-depth exploration of cybersecurity governance and information security tailored specifically for the unique challenges and responsibilities of public entities. In an era of escalating digital threats and stringent regulatory demands, establishing a robust governance framework is no longer optional but a critical necessity for government and public sector organizations. This program moves beyond theoretical concepts to deliver practical, actionable strategies for building and maintaining a secure and resilient digital infrastructure. Drawing on principles outlined by leading experts like Eugene H. Spafford and concepts discussed in seminal works such as "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman, the curriculum addresses the entire lifecycle of information security management. Participants will learn to navigate the complex landscape of public sector compliance, manage cyber risks effectively, and lead incident response efforts with confidence. BIG BEN Training Center has designed this course to empower public sector professionals with the strategic knowledge and tactical skills required to protect critical assets, ensure public trust, and uphold their duty of care in the digital age. It is an essential investment for any public entity committed to safeguarding its information and serving its constituents securely.

Target Audience / This training course is suitable for:

- Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs).
- IT Directors and Managers in the public sector.
- Information Security Analysts and Specialists.
- Government Policy Makers and Public Administrators.
- Compliance Officers and Risk Managers.
- Internal and External Auditors for public entities.
- Legal Counsel advising government agencies.
- Project Managers overseeing technology initiatives in government.
- Law Enforcement and National Security personnel.

Target Sectors and Industries:

- Federal, state, and local government agencies.
- Public education institutions, including universities and school districts.
- Public healthcare organizations and hospitals.
- Public utilities such as water, electricity, and gas providers.
- Law enforcement and emergency services.
- Public transportation authorities.
- Judicial and legal systems.
- Non-profit organizations receiving government funding.

Target Organizations Departments:

- Information Technology (IT) and Information Services.
- Cybersecurity and Information Security.
- Legal and Regulatory Compliance.
- Risk Management.
- Internal Audit and Governance.
- Public Administration and Operations.
- Finance and Procurement.
- Human Resources.
- Communications and Public Relations.

Course Offerings:

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

- Develop and implement a comprehensive cybersecurity governance framework tailored for a public entity.
- Conduct thorough risk assessments and formulate effective risk mitigation strategies.
- Navigate the complex landscape of public sector regulations and ensure compliance.
- Establish and manage an Information Security Management System (ISMS) based on international standards.
- Create and execute a robust incident response and crisis management plan.
- Enhance security for critical public infrastructure and essential services.
- Evaluate and manage third-party and vendor security risks effectively.
- Foster a strong security-aware culture across a public organization.
- Align cybersecurity strategy with the organization's public service mission and objectives.
- Communicate complex security issues effectively to non-technical stakeholders and leadership.

Course Methodology:

The training methodology employed by BIG BEN Training Center is designed to be highly interactive, engaging, and directly applicable to the professional challenges faced by participants. We believe that adult learning is most effective when it combines expert knowledge with practical application and peer-to-peer collaboration. The course will utilize a blend of instructional techniques, including expert-led presentations, in-depth case studies based on real-world public sector security incidents, and facilitated group discussions that encourage the sharing of diverse experiences and perspectives. A significant portion of the training will be dedicated to hands-on workshops and practical exercises, where participants will work in teams to develop components of a governance framework, conduct a mock risk assessment, and simulate an incident response scenario. This active learning approach ensures that participants not only understand the theoretical concepts but also gain the confidence to apply them within their own organizations. Continuous feedback from the instructor and peers is integrated throughout the course to reinforce learning and address specific challenges, ensuring a transformative and valuable educational experience for every attendee.

Course Agenda (Course Units):

Unit One: Foundations of Public Sector Cybersecurity Governance

- The unique cybersecurity landscape of public entities.
- Core principles of information security governance.
- Key differences between public and private sector security challenges.
- Legal, regulatory, and ethical frameworks in government.
- Understanding key regulations like FISMA, GDPR, and local data protection laws.
- The role of leadership and stakeholder engagement in public sector security.
- Aligning cybersecurity strategy with public service missions.

Unit Two: Developing and Implementing a Security Framework

- Introduction to major security frameworks (NIST Cybersecurity Framework, ISO/IEC 27001).
- Adapting and tailoring frameworks for public sector environments.
- Conducting a gap analysis of current security posture.
- Developing security policies, standards, and procedures.
- Establishing roles and responsibilities for security governance.
- Creating a roadmap for framework implementation and continuous improvement.
- Metrics and Key Performance Indicators (KPIs) for measuring success.

Unit Three: Comprehensive Risk Management and Compliance

- Principles of information risk management in a public context.
- Methodologies for risk identification, assessment, and analysis.
- Quantitative vs. qualitative risk assessment techniques.
- Developing a risk treatment and mitigation plan.
- Managing vendor and third-party supply chain risk.
- Strategies for continuous compliance monitoring and reporting.
- Preparing for and managing internal and external audits.

Unit Four: Incident Response and Crisis Management for Public Entities

- Building a public sector incident response plan and team.
- Phases of the incident response lifecycle: preparation, detection, containment, eradication, and recovery.
- Managing data breaches and notification obligations.
- Crisis communication strategies for stakeholders and the public.
- Coordinating with law enforcement and other government agencies.
- Conducting post-incident reviews and lessons learned sessions.
- Tabletop exercises and simulation drills for incident response readiness.

Unit Five: Securing Digital Transformation and Future Trends

- Cloud security governance for public entities (e.g., FedRAMP).
- Securing critical national infrastructure and essential services.
- Data classification and protection of sensitive public records.
- Emerging threats: AI-driven attacks, ransomware, and state-sponsored threats.
- Building a culture of security awareness across the organization.
- The future of cybersecurity governance in the public sector.
- Developing a long-term strategic vision for cybersecurity 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:

As public services become increasingly digitized, how can government entities balance the imperative for transparency and open data with the non-negotiable requirement for robust cybersecurity and citizen privacy?

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

This course distinguishes itself by its exclusive and unwavering focus on the public sector, a domain with unparalleled complexities not found in corporate environments. While other programs offer generic cybersecurity principles, this training is meticulously crafted to address the specific challenges inherent in government and public entities, such as navigating bureaucratic structures, managing tight budgets, adhering to stringent public accountability standards, and complying with a unique web of legislation. The curriculum is built around real-world case studies drawn directly from public sector incidents, providing participants with relevant, contextualized learning. Rather than just teaching theory, we emphasize the development of actionable governance frameworks and practical risk management strategies that can be implemented within the constraints of public administration. The course fosters a unique learning environment where public sector professionals can network and collaborate with peers facing similar challenges, creating a valuable community of practice. It moves beyond technical solutions to cultivate the strategic leadership and communication skills necessary to champion cybersecurity initiatives and build a resilient security culture within a public service context.