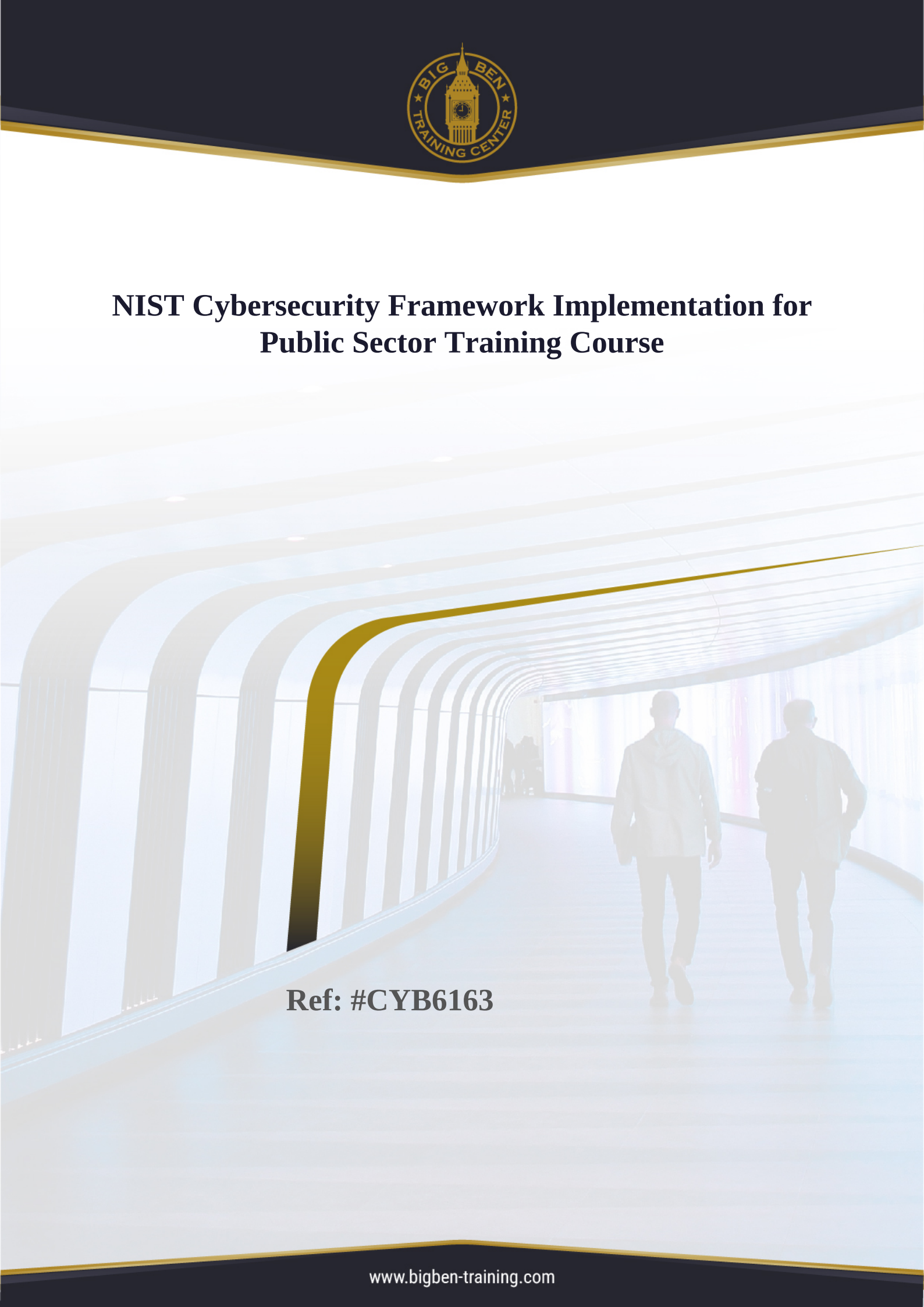
NIST Cybersecurity Framework Implementation for Public Sector Training Course



Ref: #CYB6163

Course Introduction / Overview:

This comprehensive training course is designed to provide public sector cybersecurity professionals and leaders with the essential knowledge and practical skills required to implement the NIST Cybersecurity Framework (CSF). The NIST CSF provides a flexible, outcomes-based approach to managing and reducing cybersecurity risk. While it is a voluntary framework, it has become the standard for public sector organizations seeking to improve their security posture and comply with federal mandates. This program goes beyond a theoretical overview and focuses on the practical steps needed to apply the framework's five core functions: Identify, Protect, Detect, Respond, and Recover. Participants will learn how to conduct a risk assessment, prioritize security activities, and measure the effectiveness of their program. We will cover key topics like threat intelligence, asset management, and the use of CSF to communicate risk to senior management and stakeholders. Drawing from the academic research of renowned authors like George S. Machovec and his book "The NIST Cybersecurity Framework," this program provides a strategic and practical roadmap for public sector organizations. His work emphasizes that CSF is a living document that must be continuously adapted to the evolving threat landscape. This course at BIG BEN Training Center will empower you to build a resilient and compliant cybersecurity program that protects critical public infrastructure and data.

Target Audience / This training course is suitable for:

- Public sector IT and security managers.
- Chief Information Security Officers (CISOs).
- Risk and compliance officers.
- IT auditors.
- Federal, state, and local government employees.
- Security analysts.
- Contractors working with federal agencies.

Target Sectors and Industries:

- Government agencies and equivalents.
- Defense and military.
- Healthcare and public health.
- Energy and utilities.
- Public education.
- Critical infrastructure.
- Public services.

Target Organizations Departments:

- Information Technology (IT).
- Information Security.
- Risk Management.
- Audit and Compliance.
- Legal.
- Public Affairs.
- Operations.

Course Offerings:

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

- Apply the five core functions of the NIST CSF.
- Conduct a cybersecurity risk assessment.
- Prioritizing security activities based on risk.
- Measure the effectiveness of a security program.
- Create a plan for a security incident response.
- Communicate risk and security posture to stakeholders.
- Ensure compliance with federal and state mandates.

Course Methodology:

This training course at BIG BEN Training Center uses a hands-on, scenario-based methodology that simulates the challenges of implementing the NIST CSF in a public sector environment. The program includes workshops where participants will develop a phased implementation plan for a fictional government agency. You will learn how to use the framework's tiers, profiles, and categories to create a clear roadmap for improving your security posture. The course emphasizes a practical, repeatable approach. It teaches participants to leverage the framework's flexibility to address their specific organizational needs. The instructor will provide expert guidance and feedback throughout the exercises, ensuring that you develop the critical thinking and strategic planning skills required for modern public sector security roles. This approach ensures the knowledge and skills gained are directly applicable to building a resilient and compliant security program.

Course Agenda (Course Units):

Unit One: The Foundations of the NIST CSF

- Introduction to the NIST Cybersecurity Framework.
- The five core functions: Identify, Protect, Detect, Respond, Recover.
- Understanding the framework tiers and profiles.
- Aligning the CSF with other standards.
- The benefits of using the framework.
- Communicating with stakeholders.
- Case study: a successful CSF implementation.

Unit Two: Identify and Protect

- Asset management and classification.
- Business environment and governance.
- Risk assessment and management.
- Access control and identity management.
- Data security and encryption.
- Protective technology and maintenance.
- Practical lab: a risk assessment exercise.

Unit Three: Detect and Respond

- Anomalies and events detection.
- Continuous security monitoring.
- Detection processes.
- Response planning and communication.
- Analysis of a cyber incident.
- Mitigation strategies.
- Practical lab: a security monitoring scenario.

Unit Four: Recover and Governance

- Recovery planning and improvements.
- Communication during recovery.
- Aligning recovery with business continuity.
- Framework governance.
- Integrating the CSF with enterprise risk management.
- Building a security-conscious culture.
- Case study: a post-incident recovery plan.

Unit Five: Implementation and Future Trends

- Developing a phased implementation roadmap.
- Budgeting for cybersecurity.
- Measuring program effectiveness.
- The future of the NIST CSF.
- Emerging threats and trends.
- Final project: a comprehensive CSF implementation plan.
- Continuous improvement.
- Frequently Asked Questions:

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:

The NIST CSF is designed to be highly adaptable and not a rigid checklist. However, in a public sector environment that often prioritizes compliance and checklists, how can leaders ensure the framework is used for continuous risk management and improvement rather than just a one-time compliance exercise?

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

This course stands out by providing a unique and vital focus on the practical implementation of the NIST Cybersecurity Framework, specifically for the public sector. Unlike many theoretical courses that only describe the framework, this program teaches you how to apply it to real-world government scenarios. The curriculum is built around a hands-on, roadmap-driven approach. It teaches you how to use the framework to conduct a risk assessment, prioritize security initiatives, and communicate effectively with non-technical leaders and the public. The emphasis on strategic planning, governance, and compliance within a public sector context distinguishes this course from others. It is for professionals who are ready to build a resilient and trustworthy cybersecurity program that protects critical public services.