NIST 800-53 Security & Privacy Controls Implementation

2027 □□□□□□ 10 – 6
Lisbon (Portugal)



NIST 800-53 Security & Privacy Controls Implementation

Ref: 20221771_146656 Duration: Lisbon (Portugal) Fees: 5900 GBP

Why This Course

In an era where cybersecurity threats and privacy challenges are escalating, implementing robust security and privacy controls is no longer optional — it's critical for organizational resilience. Mastery of recognized frameworks like NIST 800-53 equips professionals to protect sensitive information, manage risk, and maintain compliance across diverse environments.

This intensive 1-week program provides both the knowledge and hands-on skills needed to assess, implement, and manage NIST 800-53 security and privacy controls. Through practical exercises, case studies, and guided instruction, participants gain the expertise to apply controls effectively, tailor baselines to their organization, and establish ongoing monitoring strategies.

What You'll Learn and Practice

By attending this course, you will:

- Understand the structure, purpose, and application of NIST 800-53 security and privacy controls.
- Assess and select appropriate controls for various types of information systems.
- Implement and maintain security and privacy measures aligned with organizational needs.
- Develop strategies for tailoring control baselines and integrating hybrid controls.
- Establish continuous monitoring and improvement processes to enhance security posture.

The Program Flow

Day 1: Introduction to NIST 800-53

- Overview of the NIST 800-53 framework and its purpose.
- Understanding control families and their structure.
- Integrating controls within the Risk Management Framework.
- Practical exercise: Mapping organizational systems to NIST controls.

Day 2: Security Control Implementation

- Access control, authentication, and identity management.
- System and communications protection techniques.
- Audit, accountability, and configuration management.
- Workshop: Implementing essential security controls in practice.



Day 3: Privacy Control Implementation

- Overview of privacy control families.
- Data minimization, retention, and privacy principles.
- Individual participation, rights, and redress mechanisms.
- Conducting privacy impact assessments.

Day 4: Assessment and Authorization

- Security and privacy control assessment procedures.
- Preparing security assessment reports.
- Developing plans of action and milestones POA&M.
- Strategies for continuous monitoring and program improvement.

Day 5: Tailoring and Advanced Topics

- Tailoring control baselines to organizational context.
- Applying hybrid and common controls across systems.
- Managing supply chain risks and dependencies.
- Exploring emerging trends and future directions in cybersecurity.

Individual Impact

- Gain confidence in assessing and implementing NIST 800-53 controls.
- Develop practical skills for maintaining ongoing security and privacy programs.
- Learn to tailor frameworks to meet the unique needs of your organization.
- Strengthen your ability to monitor, evaluate, and improve controls continuously.

Work Impact

- Enhance your organization’s security posture and regulatory compliance.
- Reduce risks associated with information systems and sensitive data.
- Equip teams to implement consistent, effective, and measurable security and privacy controls.
- Build a culture of proactive security management and continuous improvement.

Training Methodology

The course combines theoretical knowledge with hands-on practice to ensure real-world application:

- Guided exercises implementing key security and privacy controls.
- Case studies illustrating control application across industries.
- Workshops for tailoring baselines and managing complex control scenarios.
- Templates, tools, and practical guidance for ongoing program management.



Beyond the Course

Upon completion, participants will be ready to:

- Assess and select NIST 800-53 controls that fit organizational requirements.
- Implement security and privacy measures effectively across systems.
- Tailor and maintain control baselines to match organizational context.
- Establish continuous monitoring and improvement programs for lasting security impact.

