QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1732

Digital Government Cybersecurity & Data Protection Training Course

DIGITAL GOVERNMENT & SMART GOVERNMENT
GOVERNMENT & PUBLIC SECTOR

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Digital Government Cybersecurity & Data Protection Training Course provides a strategic and practical framework for protecting digital government services, information systems, data assets, and citizen information against evolving cybersecurity and data protection risks. The course is designed for ministries, government entities, public-sector organizations, and institutions undergoing digital transformation and seeking to strengthen cybersecurity resilience while maintaining secure and trusted digital services.

The expansion of digital government increases the volume, sensitivity, and interconnectedness of public-sector data and systems. Government organizations must therefore address risks across digital platforms, applications, networks, cloud environments, connected systems, employees, third parties, and service providers. Effective cybersecurity and data protection require an integrated approach that combines governance, risk management, technical controls, data management, workforce awareness, incident response, and continuous monitoring.

The program covers the core principles of digital government cybersecurity and data protection, including cybersecurity governance, information security risk assessment, data classification, access management, identity security, encryption, secure digital services, cloud security, privacy protection, third-party risk, and security monitoring. It also examines practical approaches for protecting data throughout its lifecycle, from collection and storage to processing, sharing, retention, and secure disposal.

Particular emphasis is placed on managing cybersecurity incidents and protecting critical government services against disruption, unauthorized access, data loss, fraud, and other cyber threats. Participants will explore incident response, business continuity, recovery planning, security awareness, vulnerability management, and methods for strengthening organizational cyber resilience.

Through practical exercises, government-oriented scenarios, risk assessments, data protection assessments, incident response simulations, cybersecurity control reviews, and implementation planning, participants will develop the capabilities required to strengthen digital government cybersecurity and establish practical data protection measures that support secure, resilient, and trusted public services.

Objectives

- Analyze the cybersecurity challenges associated with digital government transformation.
- Assess cybersecurity and data protection risks across government systems, services, applications, and information assets.
- Develop cybersecurity governance approaches aligned with organizational objectives and digital government requirements.
- Apply data classification and data protection principles throughout the information lifecycle.
- Evaluate identity, access management, authentication, authorization, and privileged access controls.
- Assess security requirements for digital government platforms, applications, cloud environments, and connected systems.
- Apply practical approaches for protecting sensitive and personal information against unauthorized access and misuse.
- Develop cybersecurity incident response and escalation procedures for government environments.
- Evaluate third-party, supplier, and technology-related cybersecurity risks.
- Design security awareness and workforce capability initiatives to strengthen human cyber resilience.
- Develop performance indicators for monitoring cybersecurity and data protection effectiveness.
- Strengthen business continuity, disaster recovery, and cyber resilience capabilities.
- Develop an actionable roadmap for improving digital government cybersecurity and data protection.

Who Should Attend

This training course is designed for government executives, chief information and technology professionals, cybersecurity managers, information security specialists, data protection and privacy professionals, IT managers, digital transformation leaders, risk and compliance professionals, internal auditors, and government service managers.

It is particularly relevant to ministries, government authorities, public-sector organizations, and institutions responsible for operating digital government platforms, electronic services, databases, cloud environments, information systems, citizen-facing applications, and critical digital infrastructure.

The program will also benefit data managers, system administrators, network and security professionals, application and infrastructure teams, business continuity specialists, procurement and third-party risk professionals, legal and compliance teams, and decision makers responsible for cybersecurity governance, data protection, digital service resilience, and information security.

Learning Outcomes

- Explain the cybersecurity and data protection challenges associated with digital government.
- Assess cybersecurity risks affecting government systems, applications, services, and information assets.
- Develop a practical cybersecurity governance structure for digital government environments.
- Classify government data according to sensitivity, criticality, and protection requirements.
- Apply data protection controls throughout the data lifecycle.
- Evaluate identity and access management controls, including authentication, authorization, and privileged access.
- Identify security requirements for digital government applications, cloud services, networks, and connected systems.
- Assess privacy and data protection risks associated with the collection, processing, storage, and sharing of information.
- Develop practical incident response and cybersecurity escalation procedures.
- Evaluate cybersecurity risks associated with suppliers, contractors, cloud providers, and third-party services.
- Develop workforce awareness initiatives to reduce human-related cybersecurity risks.
- Establish cybersecurity and data protection KPIs and monitoring mechanisms.
- Strengthen business continuity, disaster recovery, and cyber resilience planning.
- Develop an implementation roadmap for improving cybersecurity and data protection across digital government services.

Course Outline

DAY 01

Digital Government Cybersecurity Foundations & Risk Management

- Cybersecurity in the digital government environment
- Evolving cyber threats affecting government services and information systems
- Digital government attack surfaces and critical information assets
- Cybersecurity governance, accountability, and organizational roles
- Cybersecurity risk identification, assessment, and prioritization
- Critical services, systems, applications, and information assets

> **PRACTICAL APPLICATION**
> Conduct a cybersecurity risk assessment for a selected digital government service

DAY 02

Data Protection, Privacy & Information Security

- Data protection principles and information security requirements
- Government data classification and handling
- Data lifecycle management and protection controls
- Personal, confidential, and sensitive information protection
- Data access, sharing, retention, and secure disposal
- Encryption, secure storage, and data transmission

> **PRACTICAL APPLICATION**
> Develop a data classification and protection framework for a government information asset

DAY 03

Secure Digital Services, Identity & Cloud Security

- Security-by-design for digital government services
- Identity and access management
- Authentication, authorization, and privileged access
- Application, network, and endpoint security
- Cloud security considerations for government environments
- Vulnerability management, security testing, and continuous monitoring

> **PRACTICAL APPLICATION**
> Assess the security architecture and access controls of a digital government service

DAY 04

Cybersecurity Incident Response & Organizational Resilience

- Cybersecurity incident identification and classification
- Incident response roles, procedures, communication, and escalation
- Data breaches, unauthorized access, malware, phishing, and service disruption
- Cybersecurity monitoring and threat detection
- Business continuity and disaster recovery for digital government services
- Third-party and supply-chain cybersecurity risks

> **PRACTICAL APPLICATION**
> Conduct a simulated cybersecurity incident response exercise

DAY 05

Cyber Resilience, Governance & Data Protection Roadmap

- Cybersecurity and data protection performance indicators
- Security monitoring, reporting, and management dashboards
- Cyber resilience maturity and continuous improvement
- Workforce cybersecurity awareness and capability development

DAY 05 — CONTINUED

- Cybersecurity governance, assurance, audit, and compliance
- Strategic priorities and implementation planning

FINAL WORKSHOP

Develop an integrated Digital Government Cybersecurity & Data Protection roadmap covering cybersecurity governance, risk assessment, data classification, privacy, identity and access management, secure digital services, cloud security, incident response, business continuity, third-party risk, workforce awareness, performance measurement, cyber resilience, and continuous improvement.

Register or Request More Information

Course page: https://quest-training.com/courses/digital-government-cybersecurity-data-protection-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440