Cybersecurity for M&E Databases Training Course

Professional Development Training Course Outline

Category	Monitoring and Evaluation	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the digital age, Monitoring and Evaluation (M&E) systems increasingly rely on data-driven insights to guide program decisions and policy formulations. Securing these M&E databases against unauthorized access, breaches, and data manipulation is critical for maintaining data integrity, trust, and actionable intelligence. Cybersecurity for M&E Databases Training Course emphasizes robust cybersecurity strategies, risk assessment frameworks, and proactive defense mechanisms tailored specifically for M&E environments, empowering participants to protect sensitive programmatic and beneficiary information.

Participants will explore emerging cyber threats, encryption methods, access control policies, and cloud-based security solutions, ensuring they can confidently safeguard M&E databases while complying with global data protection standards. Practical exercises, real-world case studies, and hands-on simulations are integrated to provide a holistic understanding of cybersecurity in M&E systems, enabling professionals to mitigate risks and strengthen organizational resilience.

Programme Curriculum

Cybersecurity for M&E Databases Training Course

Introduction

In the digital age, Monitoring and Evaluation (M&E) systems increasingly rely on data-driven insights to guide program decisions and policy formulations. Securing these M&E databases against unauthorized access, breaches, and data manipulation is critical for maintaining data integrity, trust, and actionable intelligence. Cybersecurity for M&E Databases Training Course emphasizes robust cybersecurity strategies, risk assessment frameworks, and proactive defense mechanisms tailored specifically for M&E environments, empowering participants to protect sensitive programmatic and beneficiary information.

Participants will explore emerging cyber threats, encryption methods, access control policies, and cloud-based security solutions, ensuring they can confidently safeguard M&E databases while complying with global data protection standards. Practical exercises, real-world case studies, and hands-on simulations are integrated to provide a holistic understanding of cybersecurity in M&E systems, enabling professionals to mitigate risks and strengthen organizational resilience.

Course Duration

10 days

Course Objectives

By the end of this training, participants will be able to:

1. Understand the fundamentals of cybersecurity in M&E contexts.
2. Identify common threats and vulnerabilities in M&E databases.
3. Implement data encryption and secure access protocols.
4. Apply network security measures for database protection.
5. Design and manage role-based access controls (RBAC).
6. Conduct risk assessments and cybersecurity audits.
7. Develop incident response and recovery plans.
8. Integrate cloud security best practices for M&E data storage.
9. Ensure data privacy compliance with GDPR, HIPAA, and local regulations.
10. Utilize monitoring tools and intrusion detection systems.
11. Apply cybersecurity frameworks like ISO 27001 for M&E.
12. Conduct penetration testing and vulnerability scanning.
13. Implement continuous security improvement strategies.

Target Audience

- M&E professionals handling sensitive program data
- Database administrators in NGOs and government agencies
- IT officers supporting M&E systems
- Program managers seeking data security knowledge
- Data analysts and statisticians
- Compliance and audit officers
- Cybersecurity enthusiasts in the development sector
- Decision-makers responsible for digital M&E infrastructure

Course Modules

Module 1: Introduction to Cybersecurity in M&E

- Key concepts of cybersecurity for databases
- Overview of cyber threats in M&E
- Importance of data integrity and confidentiality
- Case study: Breach in a health program database
- Identifying vulnerabilities in a sample M&E database

Module 2: Database Threats and Vulnerabilities

- Common database attacks (SQL injection, ransomware)

- Insider threats and human errors
- Malware targeting M&E systems
- Case study: NGO database compromise
- Threat mapping exercise

Module 3: Data Encryption and Protection

- Symmetric vs asymmetric encryption
- Encrypting sensitive M&E data
- Secure data transmission techniques
- Case study: Encrypted donor data scenario
- Encrypting sample database entries

Module 4: Access Control and Authentication

- Role-based access control (RBAC)
- Multi-factor authentication (MFA)
- User permissions and auditing
- Case study: Unauthorized access in a program evaluation system
- Configuring RBAC in a sample M&E database

Module 5: Network Security for M&E Databases

- Firewalls and secure network design
- VPNs for remote access
- Network intrusion detection
- Case study: Breach via unsecured remote connection
- Setting up a secure network simulation

Module 6: Cybersecurity Policies and Compliance

- Regulatory frameworks
- Organizational cybersecurity policies
- Data privacy principles
- Case study: Compliance failure in donor-funded program
- Drafting a security policy template

Module 7: Risk Assessment and Audit

- Identifying threats and vulnerabilities
- Risk scoring and prioritization
- Performing cybersecurity audits
- Case study: M&E system audit revealing weaknesses
- Conducting a mini cybersecurity audit

Module 8: Incident Response and Recovery

- Creating an incident response plan
- Data recovery strategies
- Communication during breaches
- Case study: Rapid recovery after a ransomware attack
- Simulated incident response drill

Module 9: Cloud Security for M&E Databases

- Cloud deployment models and risks
- Cloud security best practices
- Access and storage considerations
- Case study: Cloud breach in a monitoring system
- Securing a cloud-hosted M&E database

Module 10: Monitoring and Intrusion Detection

- Security monitoring tools
- Logging and alerting mechanisms
- Detecting suspicious activities
- Case study: Intrusion detection preventing data loss
- Configuring basic intrusion detection

Module 11: Cybersecurity Frameworks

- ISO 27001, NIST, and other standards
- Implementing frameworks in M&E organizations
- Compliance metrics
- Case study: Successful framework adoption in NGO
- Mapping database controls to ISO 27001

Module 12: Penetration Testing

- Ethical hacking basics
- Common penetration testing tools
- Evaluating system weaknesses
- Case study: Simulated attack on evaluation database
- Conducting a basic penetration test

Module 13: Continuous Security Improvement

- Security lifecycle management
- Threat intelligence and updates
- Employee training and awareness
- Case study: Continuous improvement reducing breaches
- Security improvement roadmap exercise

Module 14: Data Privacy and Ethical Considerations

- Confidentiality and ethical use of M&E data
- Legal implications of breaches
- Protecting beneficiary information
- Case study: Ethical breach in survey data
- Drafting privacy-focused data protocols

Module 15: Advanced Cybersecurity Tools and Techniques

- AI-based threat detection
- Blockchain for secure databases

- Secure API integrations
- Case study: Blockchain securing M&E data
- Experimenting with AI detection tool

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Physical	$3,000

Start Date	End Date	Location	Price
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com