Training Course on Developing a Cyber Resilience Strategy

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In an era where cyber threats are increasingly sophisticated and relentless, developing a Cyber Resilience Strategy is no longer optional—it's a critical component of organizational risk management and business continuity. Training Course on Developing a Cyber Resilience Strategy equips IT leaders, cybersecurity professionals, and decision-makers with the tools to design, implement, and sustain an effective cyber resilience framework. Leveraging the latest in AI-driven threat intelligence, risk assessment, and incident response planning, this course empowers organizations to prepare, respond, and recover from any cyber disruption.

Through hands-on learning, practical case studies, and modular instruction, participants will master the art of integrating cybersecurity best practices with business operations. With a focus on digital resilience, regulatory compliance, and adaptive security architectures, this course offers an essential roadmap for mitigating risks and fortifying digital infrastructure against evolving cyber threats.

Programme Curriculum

Training Course on Developing a Cyber Resilience Strategy

Introduction

In an era where cyber threats are increasingly sophisticated and relentless, developing a Cyber Resilience Strategy is no longer optional—it's a critical component of organizational risk management and business continuity. Training Course on Developing a Cyber Resilience Strategy equips IT leaders, cybersecurity professionals, and decision-makers with the tools to design, implement, and sustain an effective cyber resilience framework. Leveraging the latest in AI-driven threat intelligence, risk assessment, and incident response planning, this course empowers organizations to prepare, respond, and recover from any cyber disruption.

Through hands-on learning, practical case studies, and modular instruction, participants will master the art of integrating cybersecurity best practices with business operations. With a focus on digital resilience, regulatory compliance, and

adaptive security architectures, this course offers an essential roadmap for mitigating risks and fortifying digital infrastructure against evolving cyber threats.

Course Objectives

1. Understand the core principles of cyber resilience and digital continuity.
2. Design a customized resilience strategy based on your organization's threat landscape.
3. Conduct comprehensive cyber risk assessments using the latest tools.
4. Build a robust incident response and disaster recovery plan.
5. Apply zero trust architecture to your network security.
6. Integrate AI and machine learning into cyber defense systems.
7. Map your cyber resilience strategy to NIST, ISO 27001, and GDPR standards.
8. Use cyber threat intelligence platforms for proactive threat hunting.
9. Align cybersecurity goals with business continuity planning.
10. Develop an executive cyber risk dashboard for real-time monitoring.
11. Train internal stakeholders on cyber hygiene and resilience protocols.
12. Evaluate the financial impact of cyber incidents with cyber risk quantification.
13. Develop a cloud-first cyber resilience plan to secure digital transformation.

Target Audiences

1. Chief Information Security Officers (CISOs)
2. IT Risk Managers
3. Network Security Engineers
4. Cybersecurity Consultants
5. Compliance Officers
6. Business Continuity Planners
7. Cloud Security Architects
8. Digital Transformation Leaders

Course Duration: 5 days

Course Modules

Module 1: Foundations of Cyber Resilience

- Defining cyber resilience in a modern enterprise context
- Key differences between cybersecurity and cyber resilience
- Understanding resilience lifecycles
- Identifying high-impact assets and vulnerabilities
- Mapping resilience objectives to business operations
- **Case Study:** Resilience breakdown at a multinational logistics company

Module 2: Threat Landscape & Risk Assessment

- Current global threat trends and statistics
- Risk assessment frameworks (e.g., FAIR, NIST RMF)
- Identifying internal vs. external threats
- Asset classification and risk prioritization
- Leveraging threat intelligence tools
- **Case Study:** Using MITRE ATT&CK to assess financial institution threats

Module 3: Zero Trust and Adaptive Security

- Core principles of Zero Trust Architecture (ZTA)

- Micro-segmentation and continuous authentication
- Role of identity and access management (IAM)
- Behavioral analytics and adaptive controls
- Integrating ZTA with cloud and hybrid environments
- **Case Study:** Zero trust deployment in a healthcare system

Module 4: Incident Response and Disaster Recovery

- Building an incident response team (IRT)
- Playbook development and escalation protocols
- Communication strategies during incidents
- Recovery time objective (RTO) and recovery point objective (RPO)
- Post-incident analysis and reporting
- **Case Study:** Ransomware response at a global law firm

Module 5: Business Continuity and Governance

- Linking resilience with business continuity management (BCM)
- Developing resilience KPIs and metrics
- Regulatory compliance (e.g., GDPR, HIPAA, SOX)
- Data protection and privacy controls
- Cybersecurity governance models
- **Case Study:** Business continuity planning in a critical infrastructure provider

Module 6: AI, Automation & Threat Intelligence

- Role of AI in cyber defense and response
- Automated detection and response systems (SOAR)
- Predictive analytics in cyber resilience
- Building a threat intelligence feed
- Real-time alerting and automated remediation
- **Case Study:** AI-led breach detection in an e-commerce platform

Module 7: Cloud Security & Digital Transformation

- Cyber risks in cloud and hybrid environments
- Designing a cloud-first resilience strategy
- Shared responsibility model in cloud security
- Encryption, tokenization, and key management
- Securing containers and serverless environments
- **Case Study:** Cloud breach containment at a tech startup

Module 8: Human Factor & Organizational Readiness

- Cybersecurity awareness and behavior change
- Role of leadership in resilience culture
- Crisis simulation and tabletop exercises
- Internal audit and testing protocols
- Creating a resilience communication plan
- **Case Study:** Insider threat mitigation in a public sector agency

Training Methodology

- Interactive workshops with real-world scenario simulations
- Case study-based learning to reinforce practical application
- Hands-on labs using industry tools and dashboards

- Group exercises for collaborative resilience planning
- Expert-led sessions with Q&A and industry insights
- Continuous assessment through quizzes and breakout discussions

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org 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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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