NIS2 Training Course for Senior Executives

(Total: 180 minutes)

Module 1: Future Trends and Evolving Threat Landscape (15 minutes)

- **Emerging Cyber Threats:** Overview of the latest threats to the telecom industry.
- How new technologies are shaping cybersecurity.
- **Preparing for the Future:** Strategies for staying ahead of threats and ensuring security.
- Quiz 1: Quick quiz to assess understanding of evolving threats and future trends (5 minutes).

Module 2: Introduction to NIS2 Directive (15 minutes)

- **Overview of NIS2:** Evolution from NIS1 to NIS2 and why it's needed.
- **Key Objectives:** Enhancing cybersecurity across the EU and harmonizing requirements.
- **Impact on Telecom Sector:** Specific implications for telecom companies.

Module 3: Context of NIS2 in Ireland (10 minutes)

- **Irish Implementation of NIS2:** National requirements and adaptations.
- **Regulatory Bodies and Points of Contact:** Key Irish authorities involved in compliance.
- Quiz 2: Test on the understanding of NIS2's implementation in Ireland (5 minutes).

Module 4: Governance and Accountability under NIS2 (20 minutes)

- **Executive Responsibilities:** Roles of senior management in compliance.
- **Risk Management and Governance:** Integrating cybersecurity into corporate governance.
- **Board-Level Engagement:** Importance of executive-level cybersecurity knowledge.

Module 5: Key Provisions and Requirements of NIS2 (25 minutes)

- **Scope and Applicability:** Entities under NIS2 and criteria for inclusion.
- **Security Measures:** Required cybersecurity measures and incident response.
- **Incident Reporting and Cooperation:** Notification timelines and collaboration.
- Quiz 3: Quiz on key provisions and requirements (5 minutes).

Module 6: Financial and Legal Implications (10 minutes)

- **Penalties and Fines:** Financial and legal consequences of non-compliance.
- **Impact on Business Operations:** Effects on company’s operations and reputation.
- **Legal Liabilities for Executives:** Personal implications for senior executives.

Module 7: Preparing for Compliance (20 minutes)

- **Compliance Roadmap:** Steps for achieving and maintaining compliance.
- **Implementation Challenges:** Common hurdles and strategies to overcome them.
- **Leveraging Existing Frameworks:** Aligning with existing cybersecurity standards.

Module 8: Incident Response and Crisis Management (20 minutes)

- **Developing a Robust Incident Response Plan:** Key components of an effective plan.
- **Crisis Management and Communication:** Managing incidents and communication strategies.
- **Case Studies:** Lessons learned from recent cyber incidents.

Module 9: Practical Steps for Implementation (10 minutes)

- **Checklists and Frameworks:** Actionable tools for guiding compliance efforts.
- **Case Study:** Successful NIS2 Implementation: Best practices and lessons learned.
- Quiz 4: Recap quiz on practical steps and case studies (5 minutes).

Module 10: Interactive Elements and Engagement (10 minutes)

- **Interactive Scenarios and Exercises:** Role-playing exercises and decision-making scenarios.
- Polling and Surveys to gauge understanding and gather feedback.

Module 11: Executive Summary and Strategic Impact (10 minutes)

- **Executive Overview of Key Points:** Summary of critical aspects of NIS2.
- **Strategic Business Alignment:** How compliance aligns with the company’s strategy and goals.

Module 12: Conclusion and Key Takeaways (10 minutes)

- **Recap of Key Points:** Summary of essential elements of NIS2.
- **Actionable Steps:** Immediate actions for strengthening cybersecurity.
- **Q&A and Further Resources:** Providing a platform for questions and directing to additional resources.
- Final Quiz: Comprehensive quiz covering all modules to reinforce learning (10 minutes).