ISO/IEC 27001 Complemented with IEEE 1010, IEEE 1020 & Cybersecurity Value Framework (CVF)

5-Day Strategic Training Program

About the Course

This 5-day program provides a holistic and governance-focused understanding of Information Security Management by positioning **ISO/IEC 27001** as the core ISMS framework and complementing it with:

- **IEEE 1010** for ethical and professional responsibility
- **IEEE 1020** for security engineering assurance
- **Cybersecurity Value Framework (CVF)** for business value and strategic decision-making

The course bridges management systems, ethical governance, engineering assurance, and measurable business outcomes, enabling participants to view information security as a strategic business enabler.

Target Audience

- Information Security & Cybersecurity Managers
- GRC, Risk & Compliance Professionals
- CISOs, Deputy CISOs, Security Leaders
- IT & Digital Transformation Leaders
- Security Architects and Engineering Leads
- Auditors, Consultants, and Trainers
- Senior Management involved in security governance

Learning Outcomes

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

- Understand ISO/IEC 27001 as a governance-driven ISMS framework
- Integrate ethical principles into information security decision-making
- Align security engineering and assurance practices with ISMS objectives
- Explain cybersecurity controls in business value and ROI terms
- Communicate security risks and investments effectively to leadership
- Position information security as a strategic organizational capability

---

5-Day Day-Wise Course Outline

Day 1 – ISO/IEC 27001: Information Security Governance & ISMS Foundations

- Evolution of information security management
- Overview of ISO/IEC 27001 and ISO/IEC 27002
- ISMS structure and governance model
- Organizational context and stakeholder expectations
- Leadership roles and accountability
- Risk-based thinking in ISO/IEC 27001
- Information security policies and objectives
- ISMS and corporate governance alignment

Day 2 – ISO/IEC 27001: Risk Management, Control Alignment & Assurance

- Information security risk identification and evaluation
- Risk treatment approaches and control selection
- High-level understanding of Annex A controls
- Performance monitoring and measurement
- Management review and continual improvement
- Internal audits and assurance concepts
- Limitations of ISO/IEC 27001 from ethical and engineering viewpoints

---

Day 3 – IEEE 1010: Ethics & Professional Responsibility in Information Security

- Introduction to IEEE standards and their relevance
- Overview of IEEE 1010 principles
- Ethical responsibilities of information security professionals
- Responsible handling of sensitive data and monitoring activities
- Privacy, surveillance, and proportionality
- Conflict of interest and professional integrity
- Ethical considerations during incidents and breach response
- Embedding ethical governance into ISMS

Day 4 – IEEE 1020: Security Engineering & System Assurance Alignment

- Overview of IEEE 1020 and security engineering concepts
- Security considerations across the system lifecycle
- Alignment of ISO/IEC 27001 controls with engineering activities
- Security architecture and system assurance
- Validation, verification, and trustworthiness
- Collaboration between security, IT, and engineering functions
- Assurance-driven approach to resilient system design

Day 5 – Cybersecurity Value Framework (CVF): Strategy, Metrics & Business Value

- Importance of cybersecurity value in leadership decisions
- Overview of the Cybersecurity Value Framework (CVF)
- Translating security risks into business impact
- Aligning ISMS objectives with organizational strategy
- Measuring cybersecurity performance and value
- Strategic prioritization of security investments
- Communicating cybersecurity value to senior management
- Integrated view of ISO/IEC 27001, IEEE standards, and CVF

Program Takeaway

Participants gain a comprehensive understanding of how to integrate governance, ethics, engineering assurance, and business value into a cohesive information security strategy aligned with organizational objectives.