Security Risk Assessment

Day 1 – Foundations and Risk Landscape

Module 1: Introduction to Security Risk Assessments

- Purpose and value of SRAs
- Strategic vs. compliance perspectives
- Proactive vs. reactive security

Module 2: Threats, Vulnerabilities, and Risks

- Defining threats, vulnerabilities, and risks
- Categorizing threats: external, internal, emerging
- Identifying vulnerabilities: physical, procedural, cultural
- Industry-specific threat scenarios

Module 3: Legal, Regulatory, and Business Drivers

- Key compliance frameworks (HIPAA, SOX, FERPA, PCI-DSS, OSHA)
- Duty of care and litigation risks
- Insurance and liability considerations
- Strategic business benefits of compliance

Module 4: Planning the Assessment

- Defining scope and goals
- Scheduling and resource planning
- Building the assessment team (internal vs. external assessors)
- Securing stakeholder buy-in

Day 2 – Methodology, Tools, and Data Collection

Module 5: Choosing Methodology and Measurement Tools

- Qualitative, quantitative, and hybrid approaches
- Risk matrices, risk registers, gap analysis
- Scenario planning and simulations
- Benchmarking with industry standards (ASIS, ISO, NIST)

Module 6: Site Surveys and Operational Observations

- Preparing for site surveys
- Key focus areas: perimeter, entrances, interior controls, technology audit
- Observational red flags
- Staff interviews during site visits
- Documenting findings effectively

Module 7: Data Collection and Verification

- Conducting effective interviews (staff, leadership, vendors)
- Reviewing policy and incident documentation
- Pulling technical system data (access control, CCTV, alarms)
- Triangulating information to validate findings

Module 8: Threat Identification and Risk Rating

- Mapping threats to assets
- Threat modeling tools and scenarios
- Assigning likelihood and impact scores
- Prioritizing risks: accept, mitigate, transfer, avoid

Day 3 – Reporting, Implementation, and Continuous Improvement

Module 9: Reporting for Action

- Structuring the risk assessment report
- Tailoring content for executives, operations, and legal teams
- Visual aids: heat maps, scorecards, and priority charts
- Avoiding common reporting mistakes

Module 10: Leadership Briefings

- Preparing and delivering impactful briefings
- Framing risks in business terms
- Handling objections and securing approval

Module 11: Implementing Recommendations

- Prioritizing actions: critical, high, moderate, low
- Assigning responsibilities and building accountability
- Budgeting, resource allocation, and project tracking
- Training, drills, and communication strategies

Module 12: Building a Culture of Continuous Improvement

- Embedding security into daily operations
- Continuous monitoring and mini-assessments
- Encouraging reporting and feedback
- Leadership's role in sustaining security

Module 13: When Incidents Occur

- Legal and regulatory response after an incident

- Documentation as legal defense
- Crisis communication and accountability reviews
- Turning crises into catalysts for change

Module 14: Future of Security Risk Assessments

- Predictive analytics and AI in SRA
- Integrated physical-cybersecurity approaches
- Emerging trends and innovations