INFOSECTRAIN
Educate. Excel. Empower.

BATCH - 02

TPRM
Third-Party Risk Management Fast-Track Bootcamp

Hands-On TPRM for Risk & Compliance Professionals

29 - 30 August 2026

7:00 PM – 11:00 PM (IST)

8 CPEs | Scenario-Led Learning | Practitioner Toolkit | Real-World TPRM Insights

Why Attend?

Third-Party Risk Management is now essential for managing complex vendor, cloud, SaaS, AI, and fourth-party ecosystems. This fast-track bootcamp helps professionals design risk-based TPRM programs, strengthen audit readiness, track meaningful metrics, and use practical templates, checklists, and frameworks to improve governance, compliance, and executive decision-making across real-world third-party risk scenarios today.

What sets this training apart:

Scenario-Led TPRM Learning

Each module is anchored in real-world incidents or enterprise scenarios

Reusable Practitioner Toolkit

Get templates, checklists, matrices, and frameworks you can adapt

Outcome-Oriented Modules

Focus on practical implementation, not just theory

Modern Third-Party Risk Focus

Cover cloud, SaaS, AI, fourth-party, and regulatory risks

Audit & Regulator Readiness

Build evidence-based assessments and assurance practices

Career-Oriented Learning

Earn 8 CPEs, understand TPRM competencies, communication, and career paths

Participant Toolkit

- Third-Party Ecosystem Mapping Template
- Vendor Risk Tiering & Decision Matrix
- Vendor Lifecycle Governance Checklist
- Vendor Due Diligence Evidence Checklist
- TPRM KPI & KRI Catalogue
- Top 25 TPRM Red Flags & Common Failure Patterns
- Future-State TPRM Capability Roadmap
- TPRM Professional Competency Framework

Key Takeaways

Earn 8 CPEs Credits

Spot common TPRM failure patterns

Track KPIs, KRIs, and dashboards

Build audit-ready TPRM evidence

Govern vendor lifecycle effectively

Map complex third-party ecosystems

Meet the Expert

Yasesveni K

21+ Years of Experience

Corporate Trainer and Subject Matter Expert - GRC, Information Security, Cyber Security, and AI Governance | CISSP | CISM | ISO 42001 | ISO 27001 | ISO 27701 | ISO 22301 | GDPR Practitioner

Yasesveni is a subject matter expert in GRC and Cybersecurity with over 21 years of experience. She has led major security implementations and governance programs across global enterprises. She has conducted 6000+ hours of audits. As a corporate trainer, she has delivered 700+ sessions, training over 8000 participants across Asia, Europe, the Middle East, Africa, and North America in GRC, Information security, cybersecurity, and AI management systems. She combines hands-on experience in ISO standards, cybersecurity frameworks, and privacy compliance with deep experience in risk governance and digital assurance.

Her specializations include:

- Governance, Risk & Compliance (GRC) program design and enterprise risk management
- Implementation and auditing of ISO standards including ISO 27001 (ISMS), ISO 22301 (BCMS), and ISO 42001 (AI Management System)
- AI governance and risk management aligned with ISO/IEC 42001:2023
- Data protection, privacy compliance, and GDPR implementation
- PCI DSS compliance, cloud security governance, and NIST Cybersecurity Framework adoption
- Business continuity planning and operational resilience across regulated industries

Bootcamp Agenda

Day 1

Module 1: The Modern Third-Party Ecosystem

- Evolution of outsourcing and digital supply chains
- Third-party vs Fourth-party risk
- Cloud, AI and SaaS ecosystems
- Business, cyber, operational and regulatory risks
- Why traditional vendor management is no longer enough

Module 2: Designing a Risk-Based TPRM Operating Model

- Business criticality vs vendor criticality
- Risk-based assessment methodology
- Vendor segmentation and risk tiering
- Data sensitivity and regulatory exposure
- Determining assessment depth based on risk

Module 3: The Vendor Lifecycle – From Onboarding to Offboarding

- End-to-end vendor lifecycle
- Risk touchpoints at each stage
- Due diligence, contracting, onboarding, monitoring, renewal and termination
- Integrating Procurement, Security and Business functions

Module 4: Building an Audit & Regulator-Ready TPRM Program

- Evidence-based vendor assessments
- Mapping to ISO 27001, SOC 2 and regulatory expectations
- Selecting meaningful evidence
- Audit readiness and customer assurance

Day 2

Module 5: Measuring TPRM Effectiveness – KPIs, KRIs & Executive Reporting

- Defining meaningful TPRM metrics
- Executive dashboards
- Risk Committee reporting
- Program maturity indicators
- Translating operational risk into business insights

Module 6: Why TPRM Programs Fail – Lessons from Industry

- Governance failures
- Poor vendor inventories
- Assessment bottlenecks
- Vendor fatigue
- Weak contract management
- Lack of continuous monitoring
- Common audit findings

Module 7: The Future of TPRM – AI, Automation & Emerging Risks

- AI and GenAI service providers
- Fourth-party ecosystems
- Continuous assurance
- Automation in TPRM
- Emerging regulations (e.g., DORA, NIS2)
- Future operating models

Module 8: Becoming a High-Impact TPRM Professional

- Core competencies of successful TPRM practitioners
- Executive communication
- Negotiating risk with business stakeholders
- Reading contracts and assurance reports
- Career progression and professional development

Module 9: Bootcamp Wrap-Up & Practitioner Toolkit

- Key lessons learned
- Common implementation challenges
- Q&A and discussion

*Note: Participants will have access to session recordings for a period of 60 days.

Contact us

sales@infosectrain.com

www.infosectrain.com