



**SORINTEQ**

# LAW & LEGISLATION IN DIGITAL INVESTIGATIONS

A 2 day specialist training  
course for commercial  
sectors

- ✓ 2 Day Programme
- ✓ Specialist Training for Law Enforcement
- ✓ All Training Equipment Provided
- ✓ In Association With the University of Buckingham

**Contact Us**

 [0333 0063248](tel:03330063248)

 [Sorinteq Academy](http://SorinteqAcademy)



# SORINTEQ

## Course Overview

Commercial organisations conducting digital investigations operate in an increasingly complex legal environment. While businesses do not work under formal investigative authorities in the same way as Government agencies, there remains a critical requirement to understand where legal thresholds, privacy obligations, and potential authorisation issues may arise in order to avoid regulatory breaches, reputational damage, and adverse litigation.

The Law & Legislation in Digital Investigations Course is a practical 2-day intensive programme designed for commercial investigators, intelligence professionals, compliance teams, and managers responsible for internet-based investigations, due diligence, fraud enquiries, cyber investigations, and corporate intelligence gathering.

The course focuses on the legislation, regulation, and governance relevant to the private sector, ensuring learners understand how to conduct investigations lawfully, proportionately, and defensibly. It also addresses the importance of recognising where investigative activity approaches thresholds that, in Government environments, would require formal authority—allowing organisations to identify risk early and protect themselves from legal challenge.

Delivered by Sorinteq's legal lead, a qualified barrister, Doctor of Law, and experienced practitioner, the programme combines legal expertise with operational case studies and practical tradecraft considerations.

## Who is the course for?

This course is designed for commercial professionals involved in investigations, intelligence gathering, and digital risk management, including:

- Corporate investigators
- Fraud and financial crime teams
- Compliance and risk professionals
- Due diligence and corporate intelligence analysts
- Cyber security and cyber incident response managers
- Corporate security and protective intelligence teams
- Managers supervising digital investigative activity

No formal legal background is required. The course is suitable for both new investigators and experienced professionals seeking stronger legal and governance understanding.





# SORINTEQ

## Course Content

The course provides detailed legal and operational instruction across key areas, including:

- Introduction to Legal Frameworks in Commercial Digital Investigations
- Governance, accountability, and corporate investigative responsibilities
- Commercial Investigative Boundaries
- What organisations can and cannot do when conducting digital enquiries
- Understanding Authorisation Thresholds by Analogy
- Recognising where activity would require formal authority in Government settings and why this matters for commercial organisations
- Data Protection and Privacy Law
- GDPR, Data Protection Act obligations, retention, lawful basis, and handling personal data
- Surveillance, Privacy, and Human Rights Considerations
- Employee investigations, monitoring, covert enquiries, and proportionality
- International and Cross-Border Legal Considerations
- Jurisdictional risks, overseas investigations, data transfers, and operating without protective legislative authorities
- Evidence Recovery and Legal Defensibility
- Maintaining evidential integrity, defensible reporting, and disclosure considerations
- Corporate Governance and Litigation Risk
- Protecting the organisation from regulatory action, reputational harm, and civil claims
- Operational Case Studies and Legal Decision-Making
- Real-world examples of failures, litigation exposure, and successful defensible practice
- Tradecraft and Practical Application
- Using legal understanding to strengthen operational effectiveness and reduce corporate risk





# SORINTEQ

## Final Exercise Phase

- Corporate Investigation Risk Scenario
- Participants work through a realistic digital investigation involving privacy, proportionality, and legal exposure decisions
- Compliance and Litigation Review
- Applying legal reasoning to protect the organisation while achieving investigative objectives
- Debrief and Professional Review
- Structured feedback on legal defensibility, governance, and operational judgement

## Aims and Objectives of the Course

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

- Understand the legal framework governing commercial digital investigations
- Recognise legal boundaries and compliance obligations when conducting internet-based enquiries
- Understand where investigative activity may create legal exposure for the organisation
- Identify situations where Government-style authorisation thresholds would be relevant and understand the associated risks
- Apply principles of necessity, proportionality, and defensibility in corporate investigations
- Understand privacy, surveillance, data protection, and human rights considerations
- Recognise international legal risks when conducting investigations across borders
- Protect investigations, clients, and organisations from regulatory action and adverse litigation

## Why Choose Sorinteq

Sorinteq delivers university-accredited, practitioner-led training trusted by Government and commercial organisations. Our legal training ensures investigators and managers can work confidently within the law, reduce organisational risk, and maintain defensible, professional investigative standards in increasingly complex digital environments.

Students undertaking courses provided by Sorinteq may earn credits towards formal academic qualifications such as Post Graduate Certificate, Diploma or MSc at the university of Buckingham.

For further enquiries please email [info@sorinteq.com](mailto:info@sorinteq.com) or call Sorinteq on +44 (0)333 0063248.

Sorinteq provide all necessary training equipment including laptop computers, internet connectivity, mobile devices and training material.