



Regulatory Investigations & Dawn Raid Support

End-to-end support for investigations: dawn raid response, evidence gathering, and eDiscovery for Ireland's regulators and regulated entities.

Key Highlights

- We support regulators, in-house legal & compliance, external counsel and corporate investigation teams.
- Immediate response to investigations & dawn raids with forensic imaging and secure evidence handling.
- ISO27001-certified consultancy, with workflows aligned to ISO 27037 and GDPR.
- Scalable eDiscovery solutions, built for large investigations and regulatory scrutiny.
- Clear, defensible reporting and expert testimony trusted in High Court proceedings.

Our Services

Dawn Raid Support

Onsite first response, device and data triage, chain-of-custody, secure sealing and logging.

Evidence Gathering & Preservation

Tools and expertise to collect documents, records, and data (financial statements, emails, lab results, transaction logs, audit trails, etc.).

Specialists to interpret complex data.

Forensic support to ensure chain of custody and prevent tampering.

Technical Expertise in handling digital evidence (servers, cloud data, encrypted devices).

Interviewing & Witness Support

Skilled interviewers to take statements from witnesses, whistleblowers, or suspects and guidance on confidentiality if sensitive

Translation or cultural expertise if cross-border.

Privilege and Relevance Protocol

Tailored keywording and filtering, privilege logs, review sets, redactions workflows.

eDiscovery Solutions

Processing, deduplications, analytics, review hosting, technology-assisted review, and productions.

Why choose us?

- **Trusted in High-Profile Matters** - Proven expertise in regulatory and corporate investigations tested in the Irish High Court.
- **Independence & Objectivity** - We act as impartial experts, ensuring credibility with regulators and courts.
- **End-to-End Capability** - From dawn raid seizure to forensic investigations and courtroom testimony, we cover the full investigative lifecycle.
- **24/7 Availability** - Rapid mobilisation teams across Ireland to meet regulator deadlines across Ireland.
- **Operational & Logistical Support** - Project Management to track timelines, milestones, and resources and secure platforms for document management and evidence review.
- **Secure Infrastructure** - Mechanisms for data sharing that comply with privacy and confidentiality laws and evidence vaulting, encrypted data hosting, role-based access and full audit trails.
- **Cross-Disciplinary Expertise** - Forensics, Incident Response, Legal Technology, Cyber Security and GDPR compliance in one team.

Proven in Court

In ComReg v Eircom, the High Court approved regulator-led keyword searches of seized data with safeguards for privilege and confidentiality facilitated and implemented by VMGroup.

([2024] IEHC 49, 2 Feb 2024). Ruling: https://www.courts.ie/view/Judgments/b415fac0-2a8e-4245-b26a-3ce0a0a9902e/d8d38ce1-49e0-47c8-80a3-9637463c149f/2024_IEHC_49.pdf/pdf



Case Study 1 :

Commission For Communications Regulation v Eircom Limited - Regulatory Investigation – Competition & Transparency

Challenge

Commission For Communications Regulation (ComReg) is the statutory body responsible for the regulation of the electronic communications sector (telecommunications, radio communications, broadcasting transmission and premium rate services) and the postal sector in Ireland. In 2023 they initiated an investigation into Eircom Ltd following concerns about competition practices, transparency in reporting, and potential breaches of price control obligations. The investigation required urgent access to corporate records, communications, and financial data to assess compliance.

Client's Needs

- Support in conducting a dawn raid at the regulated entity's premises to secure digital evidence.
- Forensically sound seizure and preservation of data from servers, and cloud platforms.
- Efficient processing and review of large volumes of seized data to identify evidence of anti-competitive practices.
- Assurance that all evidence handling adhered to legal and regulatory standards, ensuring defensibility in court proceedings.

Solution

VMGroup deployed a specialist team to support the raid, imaging and preserving 1TB of data under ISO 27037. Using RelativityOne, deduplication methods, OCR tooling, and advanced search workflows were deployed, while maintaining a strict chain of custody and secure review environment.

Result

- Successfully secured and preserved almost 1 TB of data during the dawn raid without major business disruption at the regulated entity.
- Reduced the volume of reviewable data by 60% using deduplication, keyword searching and analytics, significantly accelerating the regulator's ability to focus on high-value evidence.
- VMGroup enabled ComReg to efficiently identify communications relevant to its statutory review of price control and transparency matters.
- Our work provided a structured, defensible evidence set for ongoing consideration in the investigation.

Case Study 2:

ODCE Fraud Investigation into Former Charity Console - Privilege & Data Protection

Challenge

The Office of the Director of Corporate Enforcement (ODCE) conducted a high-profile investigation into the affairs of the former charity Console, following allegations of financial mismanagement and governance failures. As part of the investigation, the ODCE seized large volumes of digital data belonging to the organisation. To ensure fairness and protect individual rights, an independent process was required to identify and withhold any legally privileged or personal data relating to the charity's former director before disclosure to investigators.

Client's Needs

- Appointment of an independent digital forensics and eDiscovery provider to process seized data.
- Identification and segregation of legally privileged material and personal data.
- Assurance that the ODCE would only receive data appropriate for its investigation, with no risk of infringing privilege or privacy rights.
- Clear reporting to demonstrate the independence and defensibility of the process.

Solution

VMGroup received and securely processed the data seized by the ODCE in a controlled environment, maintaining full chain of custody. VMGroup team applied advanced eDiscovery techniques to isolate potentially privileged communications (e.g., solicitor-client correspondence). Targeted searches were conducted to identify personal data belonging to the charity's former director based on subject matter and keyword phrases provided. Workflows to segregate privileged and personal materials from the review dataset were implemented.

Result

- Ensured compliance with legal privilege and data protection obligations in a high-profile, sensitive matter.
- Delivered a defensible and transparent process that stood up to external scrutiny.
- Enabled the ODCE to progress its investigation without the risk of overstepping privilege or breaching privacy rights.
- Reinforced our role as a trusted, independent service provider in regulatory and investigatory contexts.