KPMG
cutting through complexity

KPMG Forensic Technology

kpmg.ie

KPMG Forensic Technology is your reliable and experienced choice in navigating your complex unstructured data challenges.

KPMG Forensic Technology makes the digital investigation process more efficient and cost effective, while maintaining defensibility and managing current and future risks. These services integrate with KPMG's other forensic offerings, including fraud detection and anti-money laundering.

Digital Investigations

Electronic evidence gathering can be critical to the success of civil cases. Outside the courtroom, evidence gathered electronically can assist with, among other things, investigation of fraud, harassment, discrimination, employee dismissal cases and misappropriation of intellectual property.

The services offered are:


Digital Investigations


eDiscovery and Litigation Support


Cybersecurity Rapid Response

Digital investigations include the acquisition, preservation and analysis of electronic data in a manner that ensures its admissibility as evidence in a court of law.

More than ever companies are operating in a complex global business environment. They are drowning in a sea of digital data, struggling to comply with increased regulation and trying to avoid costly enforcement actions and litigation. Managing the risk of fraud and misconduct has never been more challenging.

- KPMG's Forensic Technology team has a broad spectrum of experience including Encase certified, graduate qualified and industry IT specialists. They operate in accordance with the ACPO Guidelines [1] for Electronic Evidence (on which Garda Siochana IT forensic standards are also based).
- The team interrogates various data sources to determine and prove a course of events by building a timeline of activity across single or multiple computer systems.
- The types of data sources which can be interrogated include desktops, laptops, servers, portable media, and mobile devices (such as iPads, smartphones etc.). The team is also familiar with overcoming data encryption and the technical challenges posed by it.
- Throughout each investigation the trained staff will maintain detailed notes, prepare reports, witness statements or affidavits to support the work undertaken. All such work is undertaken to a standard which is applicable to court proceedings.

Benefits to your business:

- Acquire and recover any type of electronic information from a single device to a large network environment.
- Analyse active, deleted and user-created files.
- Identify and restore the files essential for your litigation.
- Recover most password-protected and encrypted documents.
- Examine emails, Internet files and Internet history.
- Secure and provide proper chain of custody documentation for electronic evidence.
- Apply proprietary KPMG tools to perform data analysis of an organisation's books and journal entries.

Situations where this services may prove invaluable:

- Demonstrating fraudulent or criminal activity.
- Substantiating or refuting wrongful dismissal cases.
- Supporting termination with cause.
- Providing evidence of insider trading.
- Analysing data and identifying irregularities in an organisation's accounting system.
- Proving theft of trade secrets by employees or others.
- Determining an individual's activities on a network or single PC.
- Substantiating or refuting allegations of harassment.

eDiscovery and Litigation Support

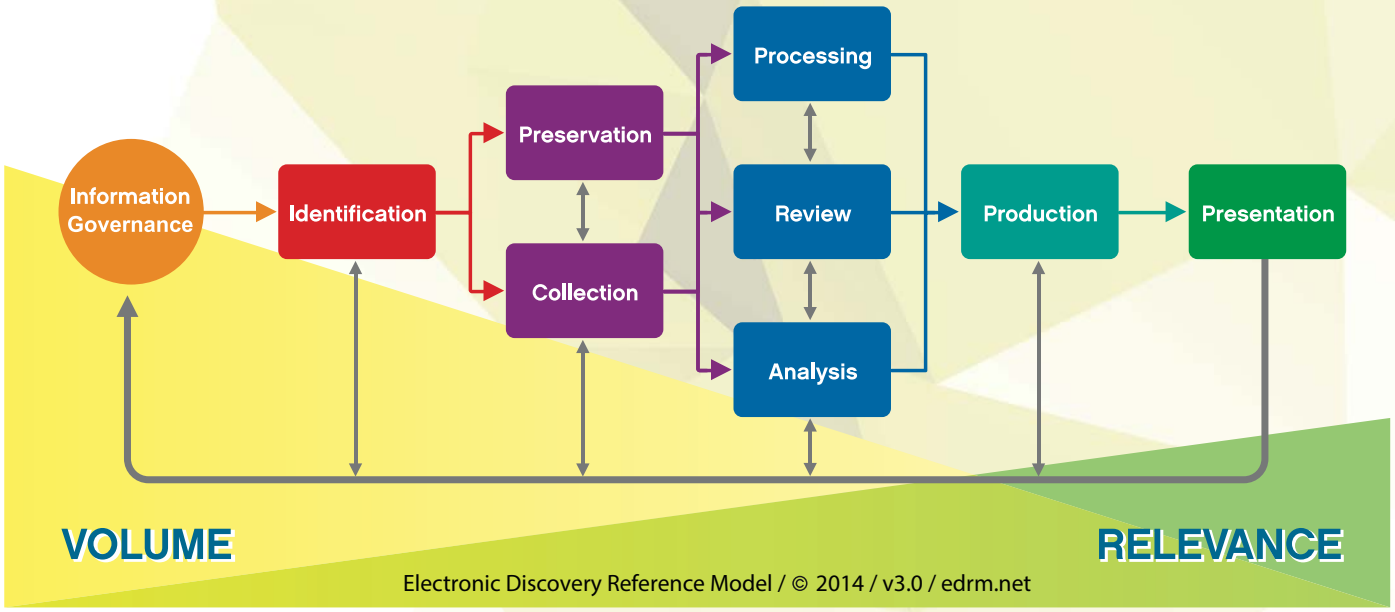
With the ever increasing amount of information that is stored electronically, advanced technology and methods need to be used to make discovery of Electronically Stored Information (ESI) manageable, this process is also known as eDiscovery.

In litigation, discovery refers to the process of making relevant documents available to the opposing legal counsel. In Ireland, S.I. No. 93 of 2009: Rules of the Superior Court (Discovery) 2009 [2], states that an order for discovery of documents could include (ESI).

KPMG has the tools and expertise to handle large and complicated eDiscovery projects. Our team uses the latest technology to greatly reduce the workload, by allowing our clients to focus on reviewing relevant documents, while we manage with the technical challenges of the eDiscovery process.

KPMG follows the Good practice guide to Electronic Discovery in Ireland (2013) [3], and adopts the Electronic Discovery Reference Model (EDRM) [4] for managing eDiscovery projects. This is a globally recognised framework, as outlined in the EDRM diagram.

Electronic Discovery Reference Model



Benefits to your business:

- A leading provider of eDiscovery services in Ireland and Europe with considerable experience in providing our expertise in small and large volume multi-jurisdictional cases.
- Access to Subject matter experts.
- A consistent high quality service with a focus on project management and clear, transparent communication.
- Services are provided under a legally defensible methodology.
- Vendor independence means we can invest in the highest quality and adaptable technologies.
- We have an extensive understanding of data privacy rules in Ireland and Europe.

"KPMG has the tools and expertise to handle large and complicated eDiscovery projects".

Cyber Security Rapid Response

For businesses today, the importance of having a secure, reliable and constantly available information infrastructures is greater than ever before. With the rise of white collar crime, criminal acts and cases of non-compliance pose significant threats.

Targeted cyber-attacks on information systems, both by internal and external perpetrators, and fraudulent activities using electronic data processing tools make the headlines almost every day. The diverse use of computer technology places high demands on measures to combat and protect a businesses' core assets from cybercrime activities.

KPMG Forensic Technology meets these demands with cutting-edge technology and an interdisciplinary team of IT specialists and investigators. With the use of the latest, internationally recognised forensic tools, combined with many years of experience in the area of digital forensics, we tackle every case with a comprehensive and targeted solution.

KPMG's four-phase case process:

Identification of Evidence

Identify the areas where electronic indications and evidence can be found, taking into account locally available data sources and network structures with external data pools (e.g. cloud services). The investigations focus on all available data storage media – from laptops to the Unix mainframe, from mobile phones to GPS devices.

Preservation of Evidence

All evidence must be inventoried and secured to preserve its integrity; the aim is to map the digital footprint in a way that is admissible as evidence in court. This can be carried out either in our Forensic Technology laboratory or directly at our clients' premises. The team locate deleted or hidden files (or fragments) and preserve evidence that the perpetrators believed to be untraceable. Neither the original data nor the systems are compromised or impaired in this process.

Presentation of evidence

The secured evidence, initially available only in electronic form, is processed in accordance with formal legal requirements and presented in a way that can be used in court. The approach and results are always clearly traceable, repeatable and transparent. A testimony from an Expert Witness can be provided if required.

Analysis of Evidence

With the use of powerful systems and tools, we analyse the secured data in KPMG's laboratory according to case specific requirements and put the jigsaw together, enabling differentiated evidence management. In some cases an initial analysis is already performed on site.

Other services offered:

- Rapid response teams to ensure the rapid preservation of data for evidential purposes
- Advanced digital forensic capability to interpret large data sets, deleted or ephemeral data in order to prove a chain of events
- Investigation into and reporting on cyber attacks for evidential or insurance purposes
- Expert witness services
- Advanced training and cyber response capability development

For more information contact:
William O'Brien | Director | Forensic Technology | william.obrien@kpmg.ie | +353 1 700 4119

References

[1] ACPO Guidelines for Electronic Evidence:
http://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

[2] S.I. No. 93 of 2009: Rules of the Superior Court:
http://www.courts.ie/rules.nsf/SuperiorAmdLookup/No31-S.I.+No.+93+Of+2009:+Rules+Of+The+Superior+Courts+%28Discovery%29+2009

[3] The Good Practice Guide to eDiscovery in Ireland:
http://ediscoverygroup.ie/Good%20practice%20guide%20to%20eDiscovery%20in%20Ireland%20v1.0.pdf

[4] Electronic Discovery Reference Model (EDRM):
http://www.edrm.net/

Key contacts

Kieran Wallace
Partner
t. +353 (1) 410 1932
e. kieran.wallace@kpmg.ie

Niamh Lambe
Director
t. +353 (1) 700 4388
e. niamh.lambe@kpmg.ie

William O'Brien
Director
t. +353 (1) 700 4119
e. william.obrien@kpmg.ie

kpmg.ie