Deloitte.

Discovery & Digital Forensics

Connecting the dots for your investigation

Forensic

Introducing our Discovery & Digital Forensics Services

Each year businesses around the world face a growing number of risks that could potentially jeopardize hundreds of billions of euros. They are victimized by fraud and theft of assets, embroiled in complex litigation or business disputes, and face accusations of financial mismanagement or malfeasance.

Among these risks, the threat of reputation-damaging legal actions is substantial. Brought by competitors, shareholders, regulators, and a company's own employees, lawsuits involving patents, large-scale class action issues, labour disputes, allegations of fraud, cyber-attacks and countless other issues can consume valuable corporate resources across legal jurisdictions and in any area of the world.

In our days, evidence in a case is not going to be primarily from tape recorders, paper documents or handwritten notes. Instead, evidence will reside in electronic format, documents, spreadsheets, emails, social media accounts, in the cloud, or moreover on smart phones and tablets (emails, instant messages, chats).

To confront these challenges promptly, businesses and their legal counsel can benefit from the assistance of our Discovery & Digital Forensic investigation professionals. Our professionals can provide many of the specialized services necessary to support a company's position and help them in their efforts to prevail.

How we can help

Deloitte Discovery & Digital Forensics helps organisations control the costs and mitigate the risks associated with the investigation process by:

- Maintaining chain-of-custody records and tracking activity to address authenticity of data and process concerns.
- Recommending and implementing solutions that fit the case at hand (and not a "one size fits all" solution).
- Coordinating investigation and discovery efforts including documentation for process reproducibility and transparent reporting.
- Applying sophisticated techniques and use of software designed to the organisation's requirements.
- Maintaining data security protocols, including the use of strong data encryption.
- Providing large-scale, redundant hosted environments for storage and access.
- Assisting companies in the development of litigation readiness programs to respond efficiently and effectively when faced with discovery requests.

Turn to Deloitte Discovery & Digital Forensics

- Our professionals utilize sophisticated technology and provide for the security and integrity of your data.
- Our team has the right mix of industry and technical experience to manage the investigation and discovery process smoothly from start to finish.
- We help our clients to manage the scope and cost of the work.
- We're nimble and able to mobilize a skilled team anywhere in the world on short notice.

The Deloitte Difference

"Connecting the dots for your investigation."

Forensic specialists. Our diverse team bring specialized technical and business knowledge. We have witnesses that have testified in court, arbitration, regulatory, and other proceedings globally.

Our experienced teams of forensic specialists have extensive technical and investigative knowledge and we have a global network of over 3000 forensic and financial crime professionals in 50 countries to assist with investigations. We bring value to our clients across numerous technical areas including forensic investigations, mobile device discovery and examinations, expert witness services and cyber incident response.

Industry-focused. Deloitte leverages in-depth knowledge of industry sectors based on years of experience working closely with our clients.

Local & Global reach. Our local team has extensive experience in local as well as global forensic engagements, and is equipped with latest technology tools, methodologies and procedures. We are also able to draw from the experience of 200,000 professionals within the network of the Deloitte Touche Tohmatsu Limited member firms and their affiliates. This access enables us to address a wide range of cross-border issues impacting people, process and technology.

Deloitte named a global leader in Forensics Investigation Consulting by Kennedy

– Kennedy Consulting Research & Advisory; Forensics & Dispute Advisory; Kennedy Consulting Research & Advisory estimates

Discovery services for nearly 30 years

6 Clients on continets

6 Industies

- Consumer & Industrial Products
- Financial Services
- Public Sector
- Technology Media & Telecommunications
- Life Sciences & Health Care
- Energy & Resources

5 Core Services


Discovery


Collections


Processing


Hosting


Review

210,000+ PROFESSIONALS

Including **800** focused on Discovery

In more than **35** Countries

Awarded Relativity's Best in Service Orange level

Achieved kCura's Orange-level Relativity Best in Service recognition for exceptional customer service.

Litigation Support

Data Collection

eDiscovery

Document Review

Expert Witness

Digital Forensics

Data Recovery

Mobile Devices Forensics

Cloud Forensics

Incident Response & Crisis Management

Incident / Crisis Simulations and War Gaming

Readiness Consulting

Malware Analysis

Our Lab & Technologies

Meet the Team

Litigation Support

A key component of litigation is the Discovery process, whereby each party provides relevant evidence to other parties in the litigation. Traditional discovery presents a risk to litigants, and, if inadequately managed, may have a significant effect on the success and cost of the litigation.

Electronic Discovery however presents an opportunity for litigants to maximise their informational, evidential and strategic advantage. In our days, evidence in a case is not going to be primarily from tape recorders, print-outs or handwritten notes. Instead, evidence will reside in electronic documents, spreadsheets, emails, social media accounts, in the cloud, or moreover on smart phones and tablets. Technology is an essential component of almost every litigation. To build a solid case and to comply with discovery rules, litigators must understand the various ways information can be stored and retrieved. Looking for a specific entry in a spreadsheet, or a single e-mail, can be daunting, but crucial. An entire business dispute or multimillion euro litigation may hinge on identifying when a single piece of data was generated – or altered, or deleted – by whom, and under what circumstances.

Today's business environment generates vast amounts of data and information. Commercial investigations and litigations increasingly rely on this data to help tell the whole story. The key to managing such huge volumes is turning the array of data into meaningful information. Lawyers must have the capability and support that's necessary for collecting this data to successfully use it in their cases.

Deloitte Discovery services were designed to manage volumes of data during investigations - whether the data is already available in electronic format or in hard copy - as well as efficiently managing all technical aspects.
Our Discovery services include forensic collection, handling, retention and analysis of data with specialised tools and methodologies in order to find information and evidence relevant to the investigation. Discovery services can be tailored to the specific needs of each litigation investigation by including only those specific phases of interest.

"While storage of data is becoming easier to manage affordably, its proliferation is a major information management and litigation risk. We are far past the days when all information potentially relevant to a matter could fit into a law firm conference room."

Data Collection

Effectively identifying and preserving data and documents to meet demands can be difficult. As such, responding efficiently, concisely and accurately to court dictated discovery or investigatory requests can raise risks. These risks can be addressed through defensible preservation methodologies and processes to help mitigate not only the risks, but also potentially reduce overall costs.

Deloitte offers data collection services across a wide range of data sources and devices. Our teams use industry standard forensic software and hardware to improve drive acquisition speed, and multiple options for write blocking to help maintain the integrity of data of each collection. Our professionals follow industry standard chain of custody (CoC) guidelines. The collection methodologies and CoC documentation are designed to meet requirements for court acceptance.

Our experience with data collection ranges from matters involving tens of thousands of data sources down to matters involving the collection of data from a single source. The data collection processes used by Deloitte can be scaled to the needs of the matter in hand. In addition, Deloitte is able to assist organizations with the development of a forensics collection work flow, collections auditing and staff augmentation needs as it relates to collections. Assisted self-collection using preconfigured devices (to collect certain folders, files types, etc.) and other remote collection services are also available as needed.

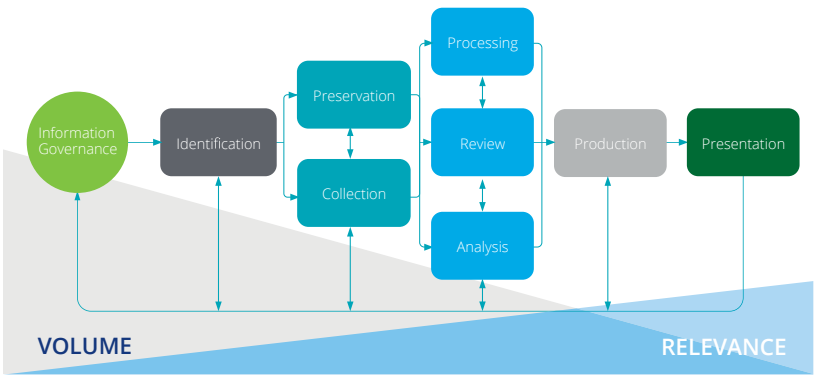
"Identifying key sources of potentially relevant information and securing your data in a sound forensic manner to ensure compliance with future proceedings".

eDiscovery

eDiscovery (Electronic Discovery) procedures are required to address regulatory authority investigations or global risks including local and cross-border disputes or international litigations. eDiscovery follows the Electronic Discovery Reference Model (EDRM), utilizing the appropriate language(s) and software. This often requires the processing of high volumes of data at a time, and requires special expertise to ensure an effective investigation.

As cross-border regulatory investigations become more prevalent, global response capability is a critical factor when selecting the experts. Our professionals provide a range of value to our clients, including their capabilities as experts, advice tailored to client's situation, and consulting on litigation readiness. Our local and geographically-dispersed laboratories and data centres provide comprehensive services within the country under investigation.

Electronic Discovery Reference Model (EDRM)



Enhancing the traditional legal process

"In a complex business dispute or regulatory investigation, all parties face one certainty: the discovery process. Deloitte's global industry and technical experience yields a more intelligent approach to discovery".


Delete
Ctrl
Alt

Document Review

Due to the rapid increase of electronic data, organizations are facing difficulties to recognize the documents required to obey with the legal proceedings requests, conduct investigations or solve business disputes. Document review is established with a detailed analysis of evidence after document and data collection.

Deloitte's Document Review professionals offer companies and their legal counsel efficient and timely assistance with document review and production in complex business disputes and investigations, including handling matters of relevance, privilege and categorization of issues. They also leverage technology and advanced analytics techniques, such as text categorization, to help create efficiencies and cost savings, protect privilege, conceal trade secrets, and comply with privacy requirements.

Reviews are usually conducted by legal personnel with Deloitte's assistance, in order to produce and privileges documents to hold back. Our team give emphasis on the document detail review, improving accuracy and generating cost savings through leading practices, workflows and provide real time response. Document review professionals also design and manage review protocols focused on protecting clients from sanctions while minimizing the costs of meeting production obligations.

"Many organizations are looking for new ways to manage document review and reign in escalating costs. Advanced analytics techniques such as predictive coding are opening the door to new opportunities for corporate legal departments, government agencies, and outside counsel looking to make sense of this growing mountain of information".

Expert Witness

Deloitte has a large-scale in professional experience for providing Expert Witness Service as part of litigation or disputes resolution in all types of disputes and industries. Law firms could use our expert witness service to evaluate the quantum of a particular claim and also to provide evidence in cases on liability involving alleged or audit neglect. Expert Witness professionals of our organisation are effective during the stages of a dispute, from counselling clients in the introductory phases to deliver expert valid evidence which could be used for a court of Tribunal.

Deloitte considers our computer forensic expert witness services as more than a transactional or one-off experience. We strive to add value through continuing education, process improvement and risk mitigation. By building long-term relationships with our clients, we are able to understand their organization and IT infrastructure and can reduce time spent repeatedly reviewing the same information. Further, we seek fee arrangements that incentivize our efficiency, while maintaining the requisite independence required of an expert witness. With the experience and help of our expert witness's professionals our clients negotiate early settlements and avoid any disruption.

"Top ranked in Global Forensics & Dispute Advisory Services, based on revenue".

Digital Forensics

Deloitte supports computer forensic-based digital investigations in a variety of fraud cases including information leakage, cyber-attack, malware incident, unauthorized access, fraudulent accounting, etc. Digital Forensics involves the securing, documentation and analysis of digital evidence from data or illicit communication. Recovering deleted and lost data, and encryption analysis, is also part of this service. Those techniques support investigations in the fields of data theft, e-mail tracing, network intrusion and intellectual property.

See beyond the matter at hand

electronic devices and networks that if required can be produced in Court. This includes hard drives (from laptops, PCs, servers etc), mobile devices, fax and printing machines and network traffic – in short, all digitally-stored data.

Computer Forensics is typically applied to isolated computer equipment where a user's actions will be tracked, such as file creation, modification or deletion of

Our forensic technology laboratory is equipped with high-end workstations and a data centre, exclusively used for investigations. This gives us the capability to effectively collect and analyze legally defensible evidence. If required, we can compile an expert opinion that can be used in Court.

"Deloitte understands that our clients face many different types of digital forensic matters. To help them address these potential challenges, our Computer and Cyber Forensics practice offers a full range of services across the forensic, discovery, and investigative lifecycles".

Data Recovery

Using the array of technology featured in our local and the worldwide network of computer forensics labs, our forensic professionals can recover a wealth of information from computer hard drives and many other media types, including active, deleted, hidden, lost or low-encrypted files, file fragments and even files that were merely viewed but never saved (memory forensics).

"Assisting clients and their legal counsel in handling large and complex data issues to help support or refute legal allegations."

Mobile Devices Forensics

Mobile devices have made a tremendous impact on the way everyday business is conducted. With increased usage of these devices in many organizations, the scope of discovery has expanded to include associated data types such as photos, voice files, text messages and application data. Additionally, detailed forensic review of the devices may allow an organization to have a broader understanding of a device's usage and attribute activities to the device's user. While the complexity of investigating mobile devices continues to rise, so does the need to investigate this media because these devices often contain critical data that may not be found in other repositories.

Deloitte brings significant experience to support mobile device management and eDiscovery solutions. In particular, we have helped many companies navigate large mobile device litigation holds, assisted with creating appropriate discovery work flows, preserved thousands of mobile devices, provided forensic analysis and reporting of devices, performed data extraction and produced mobile device data into standard review formats. Our focus is not only on collection of the mobile device, but also collecting and integrating the cellular provider records into the matter.

We have collected hundreds of mobile devices varying on different makes and models. Our teams of specialists forensically collect mobile devices using industry standard tools and protocols that are tested and verified. In addition, Deloitte has created applications to enhance the discovery capabilities beyond the use of traditional forensic tools, helping to integrate mobile device metadata and message or conversation family relationships into document review tools.

"A complete capture of mobile device data and its backups can provide an essential part of the electronic data collection for a custodian in a litigation or investigation".

Cloud Forensics

As the cloud-based productivity suite gains a strong foothold in organizations, new discovery and forensic capabilities are needed to respond to the challenges arising from this cloud computing architecture. Multiple cloud service providers with different cloud marketplace applications provide a dynamic, global environment that allows collaboration and integration with other systems. But as data leaves the enterprise, the challenges around discovery and forensics investigations can surge.

Deloitte can assist your organization by identifying and preserving data created and stored in the cloud. We work with your team to avoid disrupting active user accounts by utilizing a propriety and scalable cloud collection infrastructure. Combined with our defensible processes, we can help convert collected data into standard industry formats needed for traditional processing and review and forensic analysis.

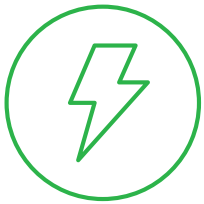
Our forensic lab has extensive capabilities that enable us to identify, collect, analyze data and support sensitive investigations in a forensically sound manner. Some of these capabilities are outlined below:

- Collection of email, e-files, documents, media, and structured data.
- Forensically sound preservation of websites, user interfaces, and API data.

"Creative.Clear.Focused."

- Analysis of cloud artefacts, metadata, and network data for investigative purposes.
- Linkage of cloud-based data with data locally collected from laptops, servers, and mobile devices.
- Social mapping and advanced analytics.

Incident Response & Crisis Management



The increase of cybercrime and data breaches continue to pose major problems for organizations in today's digital world. While adversaries can create service disruptions through cyber attacks, the most advanced methods of penetrations and breaches are specifically designed to remain undetected on your network as they collect and capture valuable data.

With cyber attacks becoming more commonplace throughout the world, responding to a data breach is not just about quickly securing your data. In addition to neutralizing threats as soon as they occur, an effective cyber incident response plan can help you understand the nature of an attack, help you reduce the cost of data loss, and introduce management rigor and controls that benefit enterprise value.

Our Solution

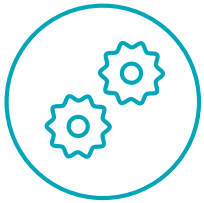
Deloitte helps organizations with incident response in their information environments to protect their important data as well as their reputations and operations. Our Incident Response practice delivers timely and actionable information as a data breach investigation unfolds so that you can make business and system protection decisions, and understand the adversaries' motives and the data they seek. Our professionals understand the uncertainties, risks, challenges and opportunities in the operating environments of large, complex organizations. Coupled with our industry experience we can deliver services, perspectives and solutions that best suit you, your business, your goals and, most importantly, your data.

Our approach to Incident Response blends deep technical skills, crisis management expertise and business intelligence to deliver a complete service, when and where organisation need it most.

"Readiness, response, recovery and a stronger future"

- Using our technical skills and field experience, forensic and "white hat" security specialists minimise the time and resources needed to find valuable digital evidence.
- Our crisis management team works with an organisation to quickly define roles and responsibilities, complete a risk and impact assessment and agree response work streams and strategies.
- Understanding your strategic business risks and organisational operations ensures that suggested response options are appropriate for your organisation.

Incident / Crisis Simulations and War Gaming



Many organizations devote substantial time and resources to risk management. But there's a place where the predictable gives way to the unpredictable - and a risk, or combination of risks, turn into a crisis. Deloitte can help your organization identify potential crises and prepare leadership, through advanced immersive training techniques, to manage a crisis.

The simulation helps lay a solid foundation for everything that follows. Theoretical threats become more real and vivid. Potential risks are more tangible and people walk away with a greater understanding of the roles they'll play when the stakes are highest.

Our approach leverages experience and innovation, applied to advanced methods of crisis simulation designed to help you understand what needs to happen during different kinds of crises, and whether your organization is prepared. So when a real crisis emerges, you not only get through it, but can emerge stronger.

A crisis simulation is an opportunity to develop capabilities, stress-test plans, evaluate coordination and communication, and preview real-time response capabilities. C-Suite executives, board members, and other key leaders are usually at the centre of the action, but the simulation should also include the larger crisis-response organization that exists behind them. Our approach is based on a distinct combination of military and academic rigor, and our own business experience. Using our advanced simulation techniques, we can assist businesses in:

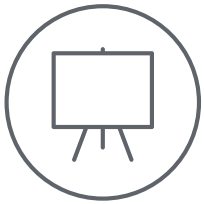
"The cyber threat landscape continues to expand rapidly. With each passing day, the cyber attacker ranks grow larger, as does their level of sophistication and the number of organizations they target".

- Understanding risks and their consequences.
- Considering worst-case scenarios.
- Aligning stakeholders and developing commitment to plans and strategy.
- Building operational readiness for new processes or structures.
- Training staff in roles and responsibilities.
- Testing plans, identifying gaps, and driving out false assumptions.
- Measuring the response capability of the organization to understand capability levels and improve response effectiveness.

Crisis simulation provides insights into an organization's readiness to manage crisis situations effectively. It is an investment that can pay off immediately, and for many years to come, if sustained through a regular and progressive program.

Not every organization can afford to have a dedicated crisis unit, or to keep one standing by. Using outside help is one way to concentrate the most experience and effectiveness into a manageable cost. Even among those who do have established crisis organizations, Deloitte's experience in running advanced simulations across hundreds of complex scenarios and industries may bring new insights and thinking to your approach—as well as the benefit of independent evaluation. Effective crisis simulation practices can help create an unforeseen advantage where organizations can transform a dangerous threat into a positive force that strengthens customer relationships, builds brand value, and enhances market perceptions.

Readiness Consulting



Preparing for the inevitable incident involves more than preparing to react - to merely neutralize a ones-off incident. It involves the ability to respond effectively and repeatedly - to plan proactively, to defend your critical assets vigorously, to get ahead of evolving threats, and to recover thoroughly when real incident do occur. As cyber attacks and other fraudulent actions increasingly take a toll on corporate bottom lines and reputations, developing a strong incident response, discovery and forensic capabilities becomes essential for businesses that seek to build secure, vigilant, resilient organizations. Such strong capabilities can help your organization:

- Quickly understand the nature of an attack - to help answer and address the questions of what, where, how, and how much.
- Minimize the costs associated with data loss - in terms of the cost of time, resources, and diminished customer confidence.
- Introduce a heightened level of management and controls that can strengthen your IT and business processes, helping your organization focus on core activities that deliver value for the enterprise.

Developing a Readiness Capability that can position your organization to meet evolving threats requires both an operational framework as well as an understanding of the incident life cycle. Building a framework and building knowledge of the phases of threat management gives your organization essential tools for proactively responding to any type of incident.

The threats and complexities of fraud and cybercrime are urgent. Deloitte proactively helps its clients to develop Incident Response, Discovery and Forensic Data Readiness capabilities so they can be ready to handle a crisis in order to emerge stronger.

"Readiness equates not only to vigilance, but also to readiness of resources.
A well prepared, multifunctional team must be poised to deal with all aspects of an incident or crisis".

Malware Analysis

Malware stands for malicious software, scripts or code meant to aid an attacker to hack a system, keep control, and steal information or to cause damage. Malware poses a large risk to an organization. At Deloitte's Forensic Malware Analysis lab, malicious software is analyzed through a root-cause oriented approach (once collected using forensically sound techniques from the organisation's environment).

Via analysing the malware using our forensic tools we can help assess whether other malware may have been also installed that could compromise the corporate systems, or whether other systems may have been similarly affected. Malware analysis is a significant ingredient of our Digital Forensics and Incident Response Services.

"Shedding light on your investigation."

Our Lab & Technologies

Effective and efficient investigations depend on establishing and maintaining a digital forensic laboratory that supports and optimizes the entire investigative process end-to-end and can withstand any evidentiary challenges. At Deloitte, we have aligned our methods and techniques with industry's forensics best practices in order to assure the authenticity, integrity and confidentiality of evidence collected for a digital forensics investigation.

Our Discovery & Digital Forensics team uses a dedicated computer forensic laboratory infrastructure as well as specialized forensic software tools and hardware field kits for national and international data collections. Furthermore, we operate a secure and efficient forensic lab facility in Cyprus, where we process structured and unstructured data for Digital Forensics and eDiscovery engagements and similar projects.

Some tools we use include:

Hard drive and loose media acquisitions	Encase, Access Data FTK, Raptor, Sumuri Paladin, Linux DD, Helix, Deft, Tableau, Hard Drive Duplicators
Network Acquisitions	Encase Enterprise, F-Response (to enable other Tools), Robocopy, FTK Imager, Linux Distros.
Mobile Device Acquisitions	Cellebrite UFED, XRY, Paraben DS, Encase Forensics
Cloud based repositories (i.e. Gmail, Facebook, Office 365, etc.)	We employee commercially available and Deloitte developed cloud collection platforms that address the majority of cloud services available in the market
Forensic Analysis & Discovery	Encase Forensics, K-Cura Relativity, Access Data Forensic Toolkit, Autopsy, Cellebrite UFED Physical Analyser, Volatility (Memory Forensics), Nuix, Proof Finder and other tools residing in Forensic Linux based distributions.

Meet the Team

Panicos Papamichael
Partner - Risk Advisory
Tel.: +357 22 360805
Mob.: +357 99 498495
Email: ppapamichael@deloitte.com

Panicos is the Partner in charge of the Risk Advisory services at Deloitte. He is a business professional with over 25 years of business experience in information security, internal audit, risk management, reengineering of business processes, information systems implementation, development of strategies, evaluation and selection of systems, organisation and operational planning and long-term business planning for clients in all major industry sectors. Panicos is a Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC) and Associate Chartered Accountant (ACA) by the Institute of Chartered Accountants in England & Wales (ICAEW). Panicos is a graduate from the London School of Economics and Political Science with a BSc (Hons) in Mathematical Economics and Econometrics.

Christos Makedonas
Manager - Risk Advisory
Tel.: +357 22 360383
Mob.: + 357 99 423842
Email: cmakedonas@deloitte.com

Christos is a Manager with our Risk Advisory department with many years of experience in the Information Security field. He is specialized in the field of Discovery & Digital Forensics, Incident Response (IR), and Cyber Risk Services. In his career, Christos was involved and lead projects including both national and international investigations in cases that involved bribery and corruption, dispute resolution, employee misconduct, data leakage, along with cases that required incident response and cyber forensics after a cyber-attack. Christos is a holder of various professional qualifications such as Certified Cyber Forensics Professional (CCFP), Certified Information Systems Auditor (CISA), Certified Ethical Hacker (CEH), Licensed Penetration Tester (LPT), Certified Malware Investigator (CMI) and Certified Security Incident Specialist (CSIS). Christos is a graduate from the London School of Economics and Polical Science, holding an MSc in Analysis, Design and Management of Information Systems and from the University of Plymouth, with a BSc in Computing Informatics (Best student price award).

Nicosia
24 Spyrou Kyprianou Avenue
CY-1075 Nicosia, Cyprus
P.O.Box 21675
CY-1512 Nicosia, Cyprus
Tel.: +357 22360300
Fax: +357 22360400
E-mail: infonicosia@deloitte.com

Limassol
Maximos Plaza, Tower 1, 3rd floor
213 Arch. Makariou III Avenue
CY-3030 Limassol, Cyprus
P.O.Box 58466
CY-3734 Limassol, Cyprus
Tel.: +357 25868686
Fax: +357 25868600
E-mail: infolimassol@deloitte.com

Larnaca
Patroclos Tower, 4th floor
41-43 Spyrou Kyprianou Avenue
CY-6051 Larnaca, Cyprus
P.O.Box 40772
CY-6307 Larnaca, Cyprus
Tel.: +357 24819494
Fax: +357 24661222
E-mail: infolarnaca@deloitte.com

Deloitte.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte Limited is the Cyprus member firm of DTTL. Deloitte Cyprus is among the nation's leading professional services firms, providing audit, tax, consulting and financial advisory services through over 550 people in Nicosia, Limassol and Larnaca. For more information, please visit the Cyprus firm's website at **www.deloitte.com/cy.**

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. Deloitte's more than 225,000 professionals are committed to making an impact that matters.

Deloitte Limited is a private company registered in Cyprus (Reg. No. 162812). Offices: Nicosia, Limassol, Larnaca.