KPMG

Forensic Readiness

Do you have a playbook for when the authorities come knocking?

kpmg.ch/forensic

This is what our clients say:[1]

[1] Study: Managing Electronic Data for Litigation and Regulatory Readiness, KPMG 2016

54%

of organizations **feel confident** of their data collection and preservation activities which may be required in the case of regulatory incidents, digital incidents or litigation. However, how can they be sure how good their activities and playbooks really are? **And what about the other 46%?**

66%

of respondents have **never undergone** a formal litigation, digital forensic or regulatory readiness assessment but **48%** think it is likely that **they will undergo** such an assessment within the next 12 months.

29%

of respondents are **concerned about the cost** of discovery as part of regulatory investigations, digital incidents or litigation, which can be especially costly when there is a review component.

How good are your playbooks to ensure that you can collect and preserve data without incurring unneccessary costs?

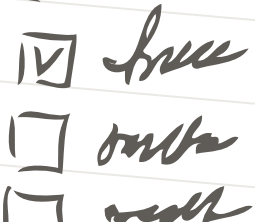
We call this digital forensic readiness

What are the main drivers for digital forensic readiness?

Data protection can be easily forgotten in times of crisis. 12% of respondents are **concerned about data protection** issues when collecting and disclosing electronic information in connection with litigation.

Stakeholders continue to have trepidation over changes in their IT environment. Among the most mentioned were "**bring-your-own-device**" policies as well as moving to "**the cloud**".

Regulations concerning data retention requirements in **different jurisdictions** are constantly changing. There are a lot of developments in the Privacy space in many jurisdictions.



Prepare Partner Evolve

Step 1 Prepare

The steps to take in response to a digital incident, litigation or regulatory data requests should be recorded in a playbook. When preparations have been done properly, your playbook will offer guidance during digital incidents or in case of raids such that your team knows who should do what, how and when.

Step 2 Partner

The impact of a digital incident, litigation, or regulatory investigation often extends well beyond your organization and could affect many stakeholders. Forging relationships with external specialists and stakeholders will work to your advantage when faced with a digital incident.

Step 3 Evolve

By learning from your own organization and from others, you can evolve your organization and thereby improve your digital forensic readiness both reactively and proactively.

How KPMG assisted clients

Improving readiness for digital incidents, litigation and regulatory investigations

Large scale litigation

A multi-national industrial manufacturing company hit with its first large-scale products liability litigation faced sanctions for its inability to timely identify and produce relevant information.

Following an assessment of the company's internal processes and procedures for identification, preservation and collection of ESI, KPMG helped the company update and establish documented, defensible processes for each phase of the eDiscovery lifecycle, and helped to ensure that the company could present not only documentation of its processes, but also evidence of their execution. In addition, KPMG helped the company better leverage its existing technology and IT resources to meet discovery requirements, while identifying areas for possible improvement through the implementation of enabling technologies.

eDiscovery readiness assessment

KPMG was engaged by a client in the public sector to assist with creating a strategy and roadmap to support the eDiscovery program.

KPMG performed data and information gathering activities designed to baseline current activities against better industry practices, including reviewing the existing protocols and data mapping activities. The client received a prioritized strategy of areas to improve the eDiscovery program which brought increased visibility into critical gaps. Those improvements included a comprehensive records management program, an organization-wide eDiscovery program, an upfront early case assessment and a greatly improved cost control.

Contact

KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich

Esplanade de Pont-Rouge 6
PO Box 1571
1211 Geneva 26

kpmg.ch/forensic

Bob Dillen
Partner,
Head of Forensic
Zurich

+41 58 249 31 11
bdillen@kpmg.com

Hedi Radhouane
Senior Manager
Forensic Technology
Geneva

+41 58 249 64 54
hradhouane@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our Privacy Policy, which you can find on our homepage at www.kpmg.ch.

© 2026 KPMG AG, a Swiss corporation, is a group company of KPMG Holding LLP, which is a member of the KPMG global organization of independent firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.