

## Drive effective investigations & compliance workflows with early, cost-effective identification of risk

- Easily connect to a variety of data sources including email servers, mobile devices, SharePoint, O365, Dropbox, and more
- Leverage AI to identify the shape and scope of risk far upstream of traditional, costly eDiscovery workflows
- Determine the presence of concepts of interest before employing keyword analysis
- Leverage previous investigations to increase the efficiency and productivity of new investigations

## Riskcovery

### By the Numbers

**3,000+**

Team members, including eDiscovery, cybersecurity, data forensics & compliance risk assessment experts

**100+**

dedicated software and database engineering and QA team for patented and patent-pending solutions development

**40+**

Brands globally leverage Riskcovery for early risk identification

### Early Risk Identification for Investigations & Compliance Audits

Successful investigations define the shape and scope of the risk exposure quickly and comprehensively. While eDiscovery provides a proven workflow, it is often too slow and expensive especially when the issues at hand are still not well known. Additional challenges arise when incorporating communication patterns of today's global commerce, involving email, mobile devices and collaboration tools like Dropbox<sup>®</sup>, O365<sup>™</sup>, and SharePoint<sup>®</sup>.

**Riskcovery is a platform designed to help investigators and compliance auditors to identify risks early, comprehensively, and cost-effectively** – enabling clients to take action to understand the risk envelope and address situations well before more formal investigations, inquiries, or audits are triggered without the traditional eDiscovery expense.

### How Riskcovery Works

**Riskcovery uses AI-driven text analytics to identify topics and concepts within documents, giving investigators a clear view into themes or trends within the data before they know what keywords to leverage:**

- Connect to popular data sources such as enterprise email platforms, Dropbox<sup>®</sup>, O365<sup>™</sup>, and SharePoint<sup>®</sup>, among others to audit data-subsets for relevance.
- Identify data populations that require special handling / forensic methods
- Review early findings and further expand or narrow the approach to achieve the optimal understanding of the risks or issues. Communications and files of material substance can be reported and exported for other workflows.
- Prioritize collection efforts and assess the most critical evidence
- Refine legal hold strategies and ensure appropriate issuance



*Proactively uncover potential investigations and compliance risks; improve adherence and enforcement of standards, including:*

- **Foreign Corrupt Practices Act**
- **Bribery Act of 2010**
- **EEOC Prohibited Practices**
- **SEC Securities Law**
- **Harassment and discrimination policies**
- **Regulations prohibiting insider trading**
- **Policies intended to prevent theft or breach of trade secrets**
- **Criteria governing deficient components, product liability, etc.**

Consilio expert advisors can also consult to create custom taxonomy templates that address your company's specific GRC requirements.

### *Early Risk Identification*

This intelligent risk management capability is at the core of our Riskcovery platform. Riskcovery is a patented, proprietary technology that uses advanced analytics to identify risk early.

Using a pre-defined taxonomy which describes specific ideas of interest, Riskcovery finds and categorizes materials with similar meaning. Riskcovery can connect to email servers and can ingest files from Dropbox, Gmail and Google Drive, or from any Windows-based file system. Additionally, ingestion of mobile device data in the form of Oxygen and Cellebrite XML files is supported.

Data Analysis with Riskcovery can dramatically sharpen the focus of internal investigations by quickly identifying potential ethical or procedural issues. Its unique analytics engine functions without the need for dictionaries or thesauri, so Riskcovery can assess documents in any language.

### *Reveal Possible Issues and Risks*

Your Riskcovery expert advisor will work with you, your Counsel, and your Compliance Officer to identify an appropriate representative sampling of corporate documents and email.

These representative samples are then imported into Riskcovery and used to identify documents that are conceptual "matches". If a customer wants to augment their samples with other related topics or samples of interest, the advisor then applies a pre-defined taxonomy to enhance assessment results. Our pre-defined taxonomies include Foreign Corrupt Practices Act (FCPA), Departed Employee Protocol and sexual harassment, or a custom template created to address your specific GRC requirements using additional documents from your own corpus, or from any data source in the world.

Documents which conform to the taxonomy concepts are categorized for further review and re-analysis. An integrated dashboard provides data visualization to reveal patterns and trends and reports can be generated to support the Riskcovery analysis and findings.

#### *CASE STUDY:*

### *Riskcovery helps drive rapid response to a DOJ Civil Investigative Demand*

A U.S.-based healthcare provider faced a Department of Justice Civil Investigative Demand (CID) investigating a claim of receiving free testing materials from a specific laboratory for quid pro quo referrals – in potential violation of the Stark Law. The client, suspecting a terminated employee had made the accusation, provided Consilio with the employee's email and laptop data for analysis by Riskcovery. Leveraging the text of the original CID along with other conceptual samples, our experts created a custom classification program for Riskcovery describing ideas of interest.

**Riskcovery identified and prioritized documents and emails conceptually similar to those in the custom classification, leading to 3,000 emails sent to a personal email account during the last three months of employment. The 2<sup>nd</sup> highest relevant document, based on the Riskcovery algorithm, was an email to the lab in question, detailing an explicit agreement to send all analyses in exchange for testing materials provided free-of-charge.** Other emails contained agreements with other labs and pharmaceutical companies as well as several including patient information – in violation of HIPAA regulations.

The client and counsel were able to justify further investigation of all of ESI and custodians identified by Riskcovery as well as assist in the development of the response to the DOJ.

**Ready to Learn More?**  
Visit [consilio.com](http://consilio.com) or email [info@consilio.com](mailto:info@consilio.com)