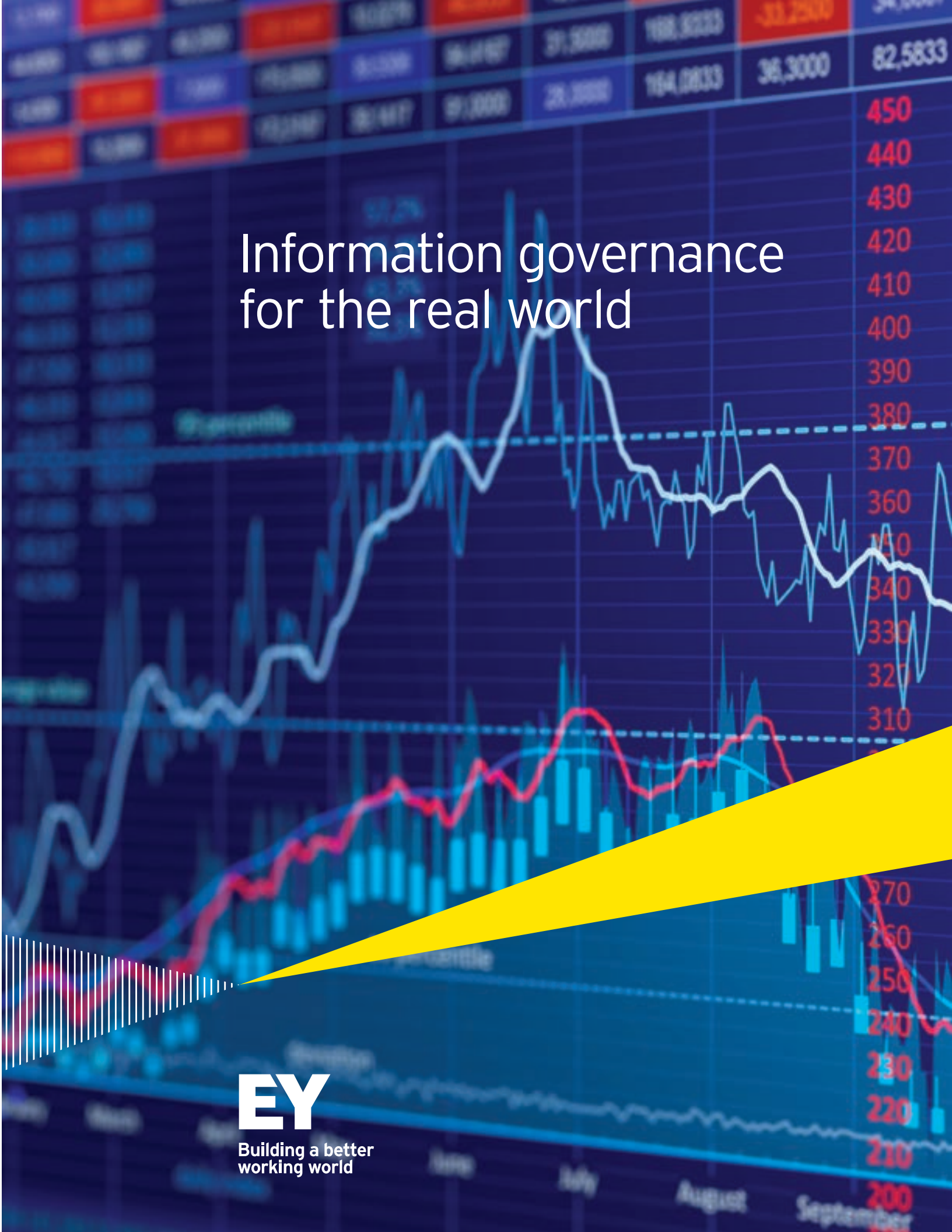


Information governance for the real world

EY

Building a better working world

"Information governance is the activities and technologies that organizations employ to maximize the value of their information while minimizing associated risks and costs."

"The Information Governance Initiative," *The Information Governance Initiative*, http://iginitiative.com, accessed January 30, 2015.

Real-world information risks span information disciplines

Recent headlines describing cyber attacks and leaked private communications make most organizations worry, "Can this happen to us?" Yet, information security breaches are just one of many information risks that companies are struggling to come to grips with.

Faced with this latest threat, will companies respond by throwing resources only at this latest challenge, or will they respond with a broader strategy that links information risks across the enterprise? Companies should ask themselves if it's time to abandon the rigid division of information risks into information disciplines — information security, privacy, records and information management, eDiscovery and so forth — and instead enable these disciplines to work together to address risks that, in the real world, span across them.

Some organizations have already recognized the need to draw together information management disciplines to better manage risks that cut across traditional organizational boundaries. Improved governance has commonly come in the form of increased cooperation between records management, legal, compliance, privacy and information technology (IT) and is spurred by, and generally related to, the mitigation of discovery risks. This is admirable, but it does not go far enough. Information disciplines responsible for structured data, data security, information access management, master data management and functions typically in IT continue to be isolated from what is, in any event, an informal arrangement between functions. Each function tackles its own information risks in its own way, often missing opportunities to leverage relevant expertise, previously completed work, and the resources and technology available in other information risk functions.

Information governance is a business issue. Organizations should have an effective information governance strategy that aligns with their overall risk management strategy, and that can be effectively operationalized to leverage and protect information assets and accomplish broader business goals.

Without the benefit of a broader understanding of the complex dependencies between risks and planned or in-flight information risk management initiatives, individual risk functions may not realize all of the available opportunities to manage information risk.

Six key considerations of a robust information governance program

The need for a strong information governance program is driven by the goals of the individual information disciplines, such as compliance with laws and regulations, protection of data, enhanced response to eDiscovery demands and achieving business imperatives. An information governance program is the glue between functions — enabling enterprise information risk management and improved coordination and cooperation between disciplines without requiring changes to the reporting structures. An information governance program, by improving risk management and coordination across information disciplines, helps companies better manage challenges, such as the following:

- **Responding to regulatory requirements.** Rigorous compliance requirements may include international standards, such as those contained in Basel III; European Union laws such as the Markets in Financial Instruments Directive; and US regulations issued by agencies such as the Financial Industry Regulatory Authority, Securities and Exchange Commission and the Food and Drug Administration. There are also a wide range of safety-related record requirements that may impact chemical, utility, oil and gas, automotive and other manufacturing companies. Among other objectives, these regulations look to protect consumers and maintain privacy rights by outlining what information organizations need to retain, how to retain the information (addressing both access and security) and what information can be transported across borders.
- **The discovery process.** Traditionally, outside counsel and third-party vendors have held a firm grip on the operations components of the discovery process. Additionally, the preservation and collection of electronic information was generally supported by corporate IT groups, which may have used a black box approach to preservation and collection of data. In recent years, judges are penalizing organizations for not taking more responsibility for their discovery process. Because of this, discovery support is shifting to its own distinct, in-house program that is in need of improved policies, procedures and controls.
- **Proliferation of systems.** Information is collected, processed and exchanged between many different internal systems, as well as external organizations (including government agencies), making understanding data flows and monitoring regulatory compliance increasingly difficult. Many organizations adopt BYOD policies and issue tablets and other portable devices, further compounding these challenges.
- **An increasing volume of information.** As the volume of information increases, so does the number of information systems

How can your information governance be improved?

- Does your organization have an information governance strategy? Are information governance objectives defined and communicated, and are resources allocated?
- Are information governance policies and procedures well defined and socialized throughout the organization?
- Does your company effectively meet legal and regulatory requirements?
- Are information governance risks considered when business decisions are made? For example, when an organization rolls out a bring-your-own-device (BYOD) technology model, are risks related to eDiscovery, records management, information security, etc., considered holistically?

and servers. As volume increases and new information systems are procured, information may shift around the country or globe. As this happens, organizations tend to lose their understanding and control of what information is stored where. This presents risks when an organization must apply records retention policies, respond to discovery or regulatory requests, determine compliance with privacy requirements, etc. If companies cannot identify data and dispose of it in accordance with retention policies, then that data may be discoverable and increase eDiscovery risks and costs.

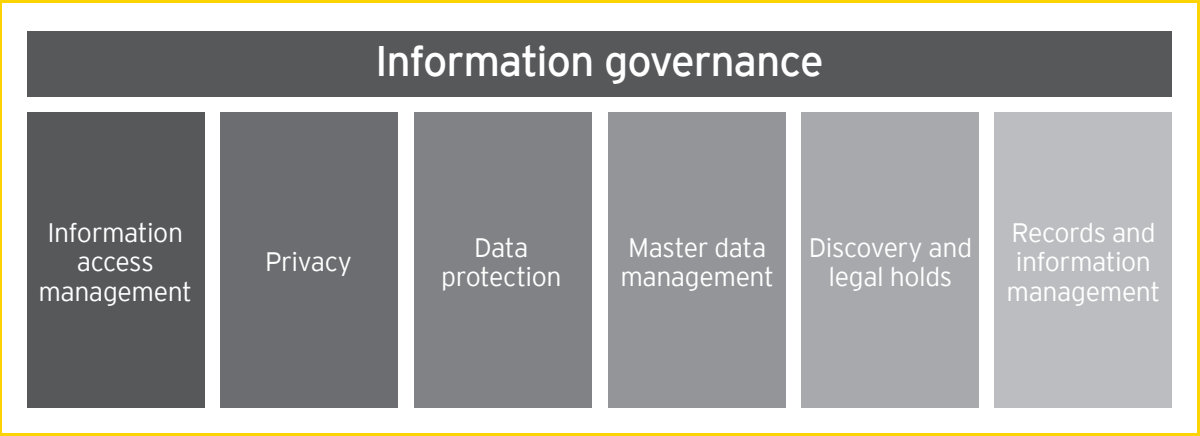
- **Increased risk of cyber attacks.** Publicized cyber events amplify the risks to all organizations trying to protect their critical information. The resulting loss of trust and reputational damage has led to economic and revenue hits for both small and multinational organizations. Without knowledge of an organization's critical assets, too many resources are spent on protecting everything. While there are many ways to gain access to an organization's environment, whether through third-party vendors with too much access or social engineering of the front line, the goal is to build up defenses around those critical assets.
- **Outsourcing.** Outsourcing IT services, including to offshore locations, increases both security and compliance risks. Third-party service and infrastructure providers outside of the organization that have custody of the organization's information may not have appropriate protections or information governance capabilities in place.

True information governance is a program

Information governance is not a project or an information management discipline – it enables information management disciplines to be managed holistically. Through its information governance program, the organization can better understand and address enterprise information risks.

The emphasis in information governance is squarely on "governance."

The information governance program does not replace existing information disciplines or reporting structures for those disciplines, but establishes shared governance and a culture of coordination and integration between disciplines.



How we can help

Ernst & Young LLP works with organizations to find opportunities to mitigate overlapping risks by bringing these siloed functions together. When organizations implement a well-balanced information governance program, they can better identify effective approaches to managing and mitigating enterprise information risks.

- **Information governance program assessment and strategy development diagnostic.** Ernst & Young LLP employs a diagnostic that is based on the four foundational components of our information governance framework: strategy, governance, operations and performance measurement (see graphic on page 6). By observing and evaluating the organization's current approach to information risk across disciplines, the organization begins to understand the current state of its information governance program and can plan for its desired future state. The diagnostic identifies risks across the spectrum that can be aligned to recommendations for improvement.
- **Information governance program maturity model.** The information governance diagnostic described above can also be used to develop a profile of the organization's information governance program and its maturity compared with other organizations in the same industry. The maturity model

may also reflect the organization's desired future state and depict the gaps that must be closed to achieve the future state.

- **Information governance program development.** We work closely with organizations to help them realize their future-state information governance programs. This work can involve establishing a committee that includes executives from the various information management disciplines and other stakeholders; working with stakeholders to develop or streamline corporate strategy, policies, procedures, standards, reporting and controls to support the revised program and its initiatives;

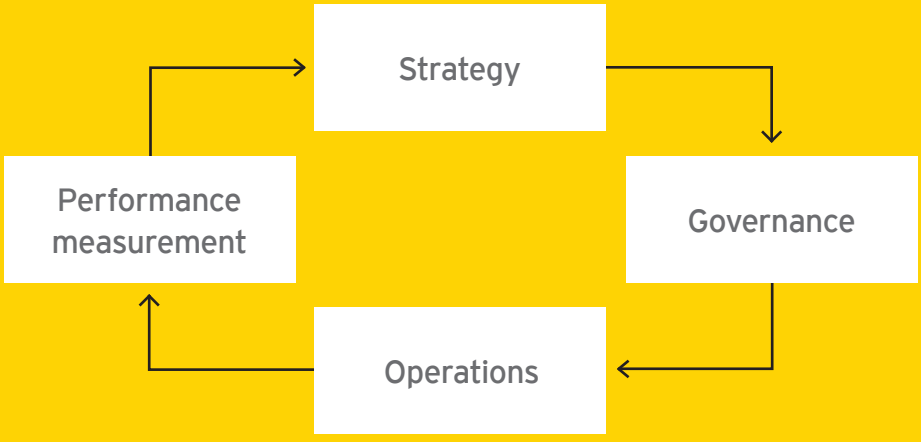
The four components of our shared-focus framework provide an effective design and solid foundation for implementing a sustainable information governance program.

Strategy: This describes how information governance will help realize the business strategy, facilitate compliance with applicable regulations, improve operations, manage risk and improve the organization's economic position.

Governance: This includes defining the information governance organization and the ongoing maintenance, administration and safekeeping of the information governance program.

Operations: This comprises the infrastructure, systems and processes that make the information governance program operational.

Performance measurement: This consists of assessing how well information governance is performing against the needs of the business and expectations of the users.



developing change management plans to prepare employees for changes to the information governance program; helping implement training programs to socialize the new model and policies; and more.

- **Regulatory review.** As regulations continue to change and emerge, it can be difficult for organizations to understand whether their businesses are compliant with applicable laws. We work with clients to evaluate the information governance program's compliance with regulations promulgated globally. Additionally, once applicable regulations are identified and compliance with those regulations has been evaluated, organizations may need to refine or enhance their programs to implement appropriate controls to improve compliance.
- **Data maps.** With the explosion of information retained by organizations, it is becoming increasingly burdensome and difficult to locate records and information and respond to regulatory or litigation requests efficiently. We work with organizations to develop data maps that align regulated records to their system of records or repositories. These data maps can also be used to identify where other information that is frequently subject to discovery is stored, easing preservation and collection.
- **Develop discovery preparedness plan.** Our teams work closely with discovery and legal support teams to develop a "discovery playbook" to guide preparedness for discovery. This playbook is composed of standardized procedures and reports, and acts as a blueprint for the operational elements of discovery. The standard procedures contained in the playbook may describe how the discovery or legal support team executes and oversees the identification, preservation, collection, processing, review, analysis, production and presentation of information subject to discovery requests. The standardized reporting templates are used to memorialize the decisions made and activities performed when responding to requests. This discovery playbook allows organizations to execute discovery consistently, facilitates the transfer of knowledge to new resources, increases the level of transparency and quality control when working with third-party vendors, and increases the defensibility of the organization's discovery function.
- **Understanding critical assets.** Organizations create information that can become vulnerable whether it is active or inactive, on-site or in the cloud. Organizations are struggling with information overload, the cloud, remote workforces and BYOD. Just understanding where information is and what should be protected is a major challenge.

Ernst & Young LLP works with organizations to catalog data assets and determine the necessary steps for managing information security risks. Knowing where the critical information is stored, and how it is stored, is fundamental to information security, as well as other information management disciplines.

- **Data protection.** We work with clients to design and help implement strategies for safeguarding data, information and records, as well as improving business processes and information security, to reduce the risk of data breaches and strengthen the detection of leaks.
- **Designing and implementing training programs.** A training program can help educate employees about information governance policies and procedures. Program content may vary according to the level of employee and their degree of involvement in the program. We work with clients to develop and deliver effective training programs.
- **System selection and implementation support.** Systems that support the management of information must consider requirements that cross information management disciplines. We help companies plan their approach to system selection, the development of scoring and weighting models, and the identification of business and function requirements. We also assist with the pilot of their leading candidates.
- **Developing a defensible disposition program.** Defensible disposition is the process of identifying and disposing of records, documents and data in a manner consistent with the company's own document retention policies and applicable laws and regulations. By implementing an effective defensible disposition program, organizations can reduce IT costs, reduce litigation risk and avoid potential discovery costs. The goal of an effective defensible disposition program is to classify and then dispose of data in accordance with retention and legal hold policies to reduce corporate risk and control legal and business costs.

Effective information governance helps the organization reduce costs, demonstrate compliance, protect rights, defend against claims and improve operations. The traditional model of siloed functions that manage vertical information governance disciplines is shifting to a more integrated, collaborative format better suited to managing information risk. When these functions understand and approach risks together, the organization is stronger and better positioned to manage the ever-increasing volume of information, reduce costs and prepare for the future.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about ourorganization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY's Fraud Investigation & Dispute Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority—no matter the industry sector. With our more than 3,200 fraud investigation and dispute professionals around the world, we assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. And we work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

1501-1382586
EYG no. WW0376

ED none

ey.com