Cybersecurity reporting: Now, next and beyond

Disruptive technology is changing the game for cybersecurity and risk management leaders, just as it is for business and functional leaders. Artificial intelligence (AI), blockchain, robotic process automation (RPA) and the cloud are changing how companies operate and engage with customers, whose expectations for speed, transparency and personalization are constantly increasing. These changes in technology and customer expectations can create new vulnerabilities.

Beyond the need for companies to detect, repel and recover from increasingly sophisticated threats, there is growing need for organizations to report to their management, boards and outside stakeholders (such as shareholders) on how the organization is being protected from the growing rates of cyber attacks.

In addition to building stronger defenses and locking down assets and creating latency issues, cybersecurity leaders are seeking to embed leading-edge security practices and risk intelligence deeply within key operations and processes. Models such as Trust by design (see text box for an explanation) is an approach that can both enrich relationships with customers and strengthen protections for digital assets and their associated brand. Trust by design reflects the idea that digital security is an enabler of – rather than a barrier to – growth.

Trust by design is our adaptive risk management approach to clients' growing demands for advice on how they can embed trust as a design principle into their businesses. Trust by design helps financial services firms become digitally confident and trusted enterprises that have the intelligence and insights to drive growth, increase business value and maintain stakeholder trust.

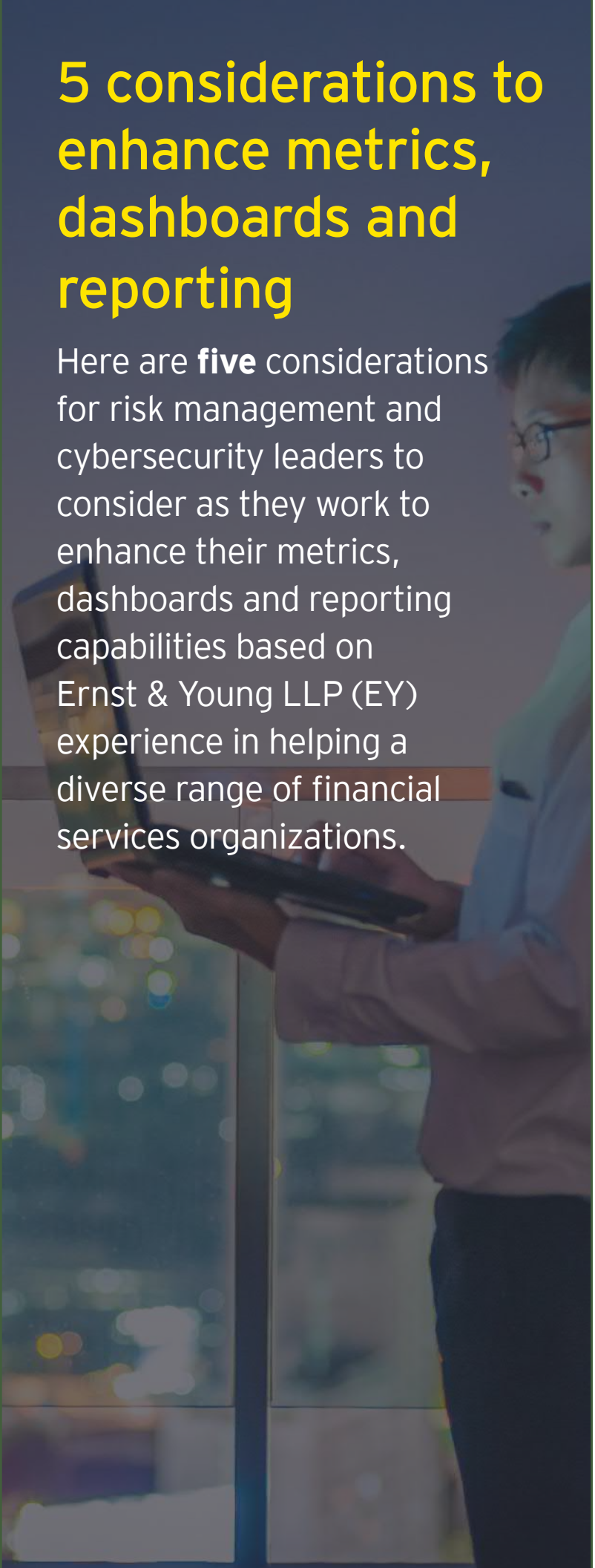
Discover more by visiting our collection of insights about Trust by design.

As these practices mature, risk management and cybersecurity leaders are also challenged to define and deliver the right risk and performance metrics, dashboards and reports. Specifically, they must enhance the quality and integrity of data and educate the business on what metrics matter and why they matter – and do so with the urgency today's consumers demand.

EY
Building a better working world

5 considerations to enhance metrics, dashboards and reporting

Here are **five** considerations for risk management and cybersecurity leaders to consider as they work to enhance their metrics, dashboards and reporting capabilities based on Ernst & Young LLP (EY) experience in helping a diverse range of financial services organizations.



1 It's all about the metrics

Board members and business stakeholders need to see risk metrics in a context they can understand, such as cost and operational impacts (e.g., downtime associated with certain security events). The strongest metrics don't just relate what happened, but also "tell a detailed story," reflecting both what has occurred (recent events and trend lines) and where the organization is going (relevant forecasts). Probability estimates relative to security events can be an effective metric for capturing the attention of business leaders.

Beyond communicating how many breach attempts the company experiences, metrics should highlight how quickly the breach attempts were detected, how resilient the organization is in terms of repelling them and how effectively the organization is in recovering after the breach has been detected. Better still, metrics can suggest or promote effective actions (e.g., by identifying preventive steps the business can take to further strengthen protections). Ideally, key risk indicators (KRIs) would be closely linked to key performance indicators (KPIs) for the business.

In terms of the specific KPIs that actually present such a fulsome picture, they will vary by organization, depending on business model, product portfolios, customer segments and other factors. However, most organizations will need a combination of top-down and bottom-up metrics, including those that address the needs of different levels of the organization. (Refer to the text box on page 4.) For example, aggregated high-level metrics should help provide answers to questions the board and senior business leaders are likely to ask. More detailed operational metrics are necessary to inform, educate and enable domain, functional and business line leaders.

2 Implement product and service management

Most financial services firms already use dashboards, including "red-yellow-green" formats. While these provide easy-to-understand, "snapshot" views of data, they may not be fully understood by board members or business stakeholders. The key is educating those groups on what the metrics mean, so directors can ask the right questions related to issues identified by the data (see the next point), which in turn helps instill a more risk-aware culture.

Dashboards can help show progress in the use of higher quality or more timely data. It's never too late to build a better dashboard or consolidate existing ones. In other words, smarter dashboards clearly illustrate the value of better data and metrics.

Providing access to "drill-down" data and detailed metrics that are aggregated around specific categories can support the needs of different parts of the organization. For example, the likely scope and severity of insider threats and the organizational ability to detect them should be measured within the context of a broader threat management program and in terms of specific external threats. Refer to the text box below.

Avoid reporting for reporting's sake. That is an important rule of thumb embraced by many cybersecurity veterans. Generally speaking, there is greater risk in reporting too much data rather than too little; for example, metrics that don't change over time may not be worth reporting at all. Benchmarking data and leading practices could help clarify the best metrics. The more data and dashboards are tailored and "right-sized" for specific audiences, the more effectively they are able to communicate the organization's cybersecurity status.

It is also important to recognize that boards and senior management are increasingly getting differing views on cybersecurity from within their company. The chief information security officer (CISO) is no longer the only source of cyber KRIs. Second-line risk management is also creating their own view of risk across the organization. The third line – internal audit – will also provide a view on the quality of cyber risk management. While these differing perspectives are more powerful for being independent of each other, it is important that management helps the board appreciate how these risk perspectives fit together.

Looking for the right metrics for your dashboard? Think both top-down and bottom-up

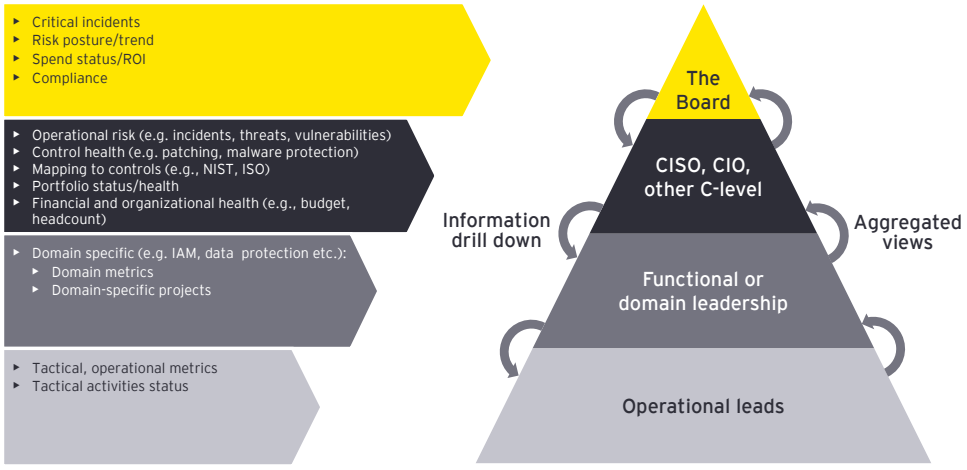
Risk management teams serve multiple constituencies across the organization, each with different informational needs and unique responsibilities. That's why dashboards must be designed flexibly, so that different user groups can access the cybersecurity metrics they need to make decisions and fulfill their responsibilities.

For instance, boards will be interested in high-level, strategic perspectives, with views to overall cyber-risk posture and trends, financial information (such as current spend levels and returns on previous investments) and compliance and regulatory status.

Chief information officers and CISOs will want more granular views that speak to specific operational risks, controls (both internal, such as patching against the latest malware, and industry standards, such as NIST and ISO) and organization metrics relating to budgets and headcounts.

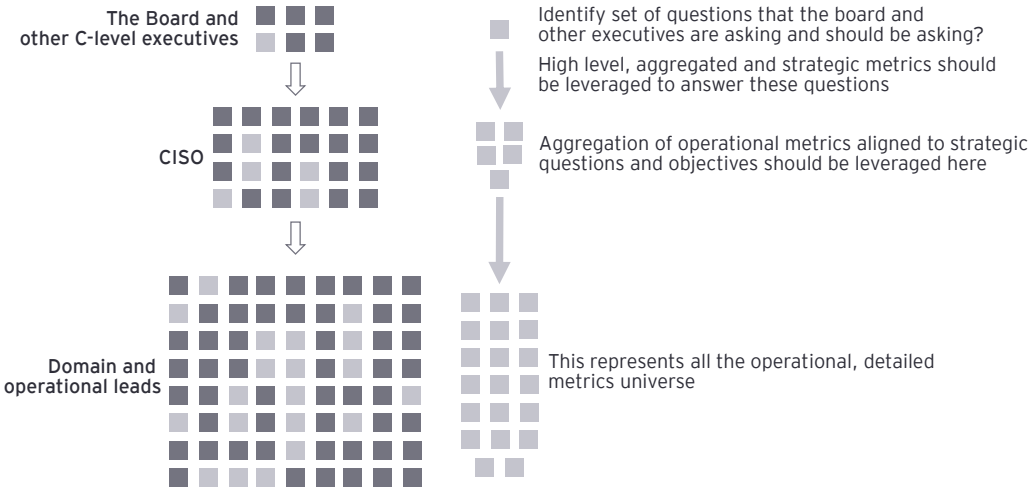
Going further down and out in the organization, business leaders will be focused on domain-specific metrics (such as identity access management and data protections) and the status of tactical activities.

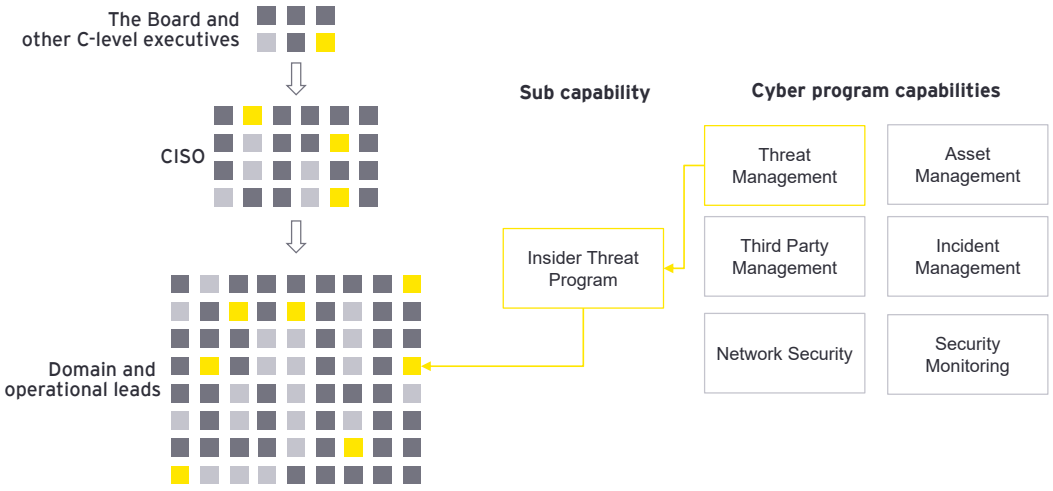
The most effective dashboards provide critical security metrics that speak to different audiences and users from different parts of the organization

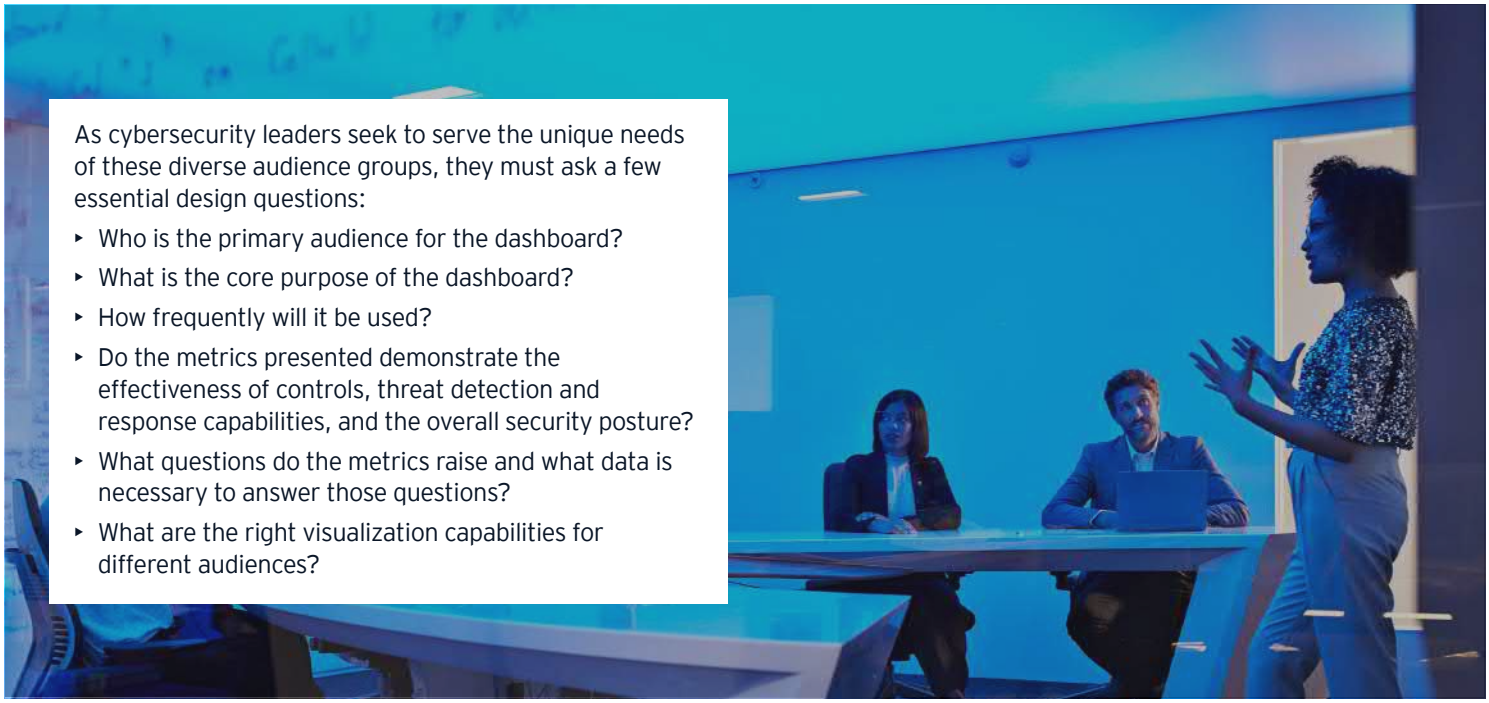


1. National Institute of Standards and Technology (NIST) is a non-regulatory federal agency under the Department of Commerce. Their mission is to develop and promote measurement, standards and technology to enhance productivity, facilitate trade and improve the quality of life.

2. The Information Services Office (ISO) is responsible for creating, maintaining, and disseminating a NIST knowledge base which supports the research and administrative needs required to fulfill the scientific, engineering, and technical mission of NIST.







As cybersecurity leaders seek to serve the unique needs of these diverse audience groups, they must ask a few essential design questions:

- Who is the primary audience for the dashboard?
- What is the core purpose of the dashboard?
- How frequently will it be used?
- Do the metrics presented demonstrate the effectiveness of controls, threat detection and response capabilities, and the overall security posture?
- What questions do the metrics raise and what data is necessary to answer those questions?
- What are the right visualization capabilities for different audiences?

3 Significant data challenges remain

Data accessibility, quality and reliability will determine how effective metrics and even the best-designed dashboards can be depended upon. Most businesses have room for improvement in these areas. Even senior security professionals spend too much time hunting for data and reworking spreadsheets to get the views they need. Data quality issues affect business stakeholders, too. When there is low confidence in underlying data, executives will be skeptical of metrics and reports.

At the largest organizations, it's difficult to assess the completeness of controls because not all business units, product lines or functions integrate their data with enterprise systems. It's common for security teams to uncover unknown data sources. Still, reporting with imperfect data can be a catalyst for change. Stakeholders then understand the limitations of data and the urgency to act to upgrade quality and access.

There is a clear and pressing need to increase the confidence level in data integrity. Increased automation, which can streamline data collection, enhance data quality and free time for higher-value analytical work, should be a priority for risk and cyber teams. Experience gained from EY professionals indicates that automation delivers significant value in dramatically reducing manual effort, even if it requires the "heavy lifting" of restructuring repositories or re-engineering processes.

4 Education, communication and contextualization are big parts of the job

Even well-defined, digestible metrics and the sharpest dashboards may need to be contextualized for the business. Board members and business stakeholders must understand both *what metrics mean* and *why they matter*. This is especially important given the speed at which new threats emerge and existing risks mutate.

Further, they need confidence that the data underlying the metrics is trustworthy. For instance, tracking the number of cyber attacks and how many have been successfully repelled is somewhat useful, but not necessarily meaningful in highlighting the company's ability to resist or recover from the most serious attacks.

These are among the first steps to building more mature "risk cultures" in which everyone – on the first, second and third lines of the business – recognizes that they have a role to play in securing assets and protecting the reputation of the business.

5 Think bigger – and differently – to enable trust by design

Reporting metrics and engaging the business remain atop the agenda for cybersecurity teams, but forward-looking leaders are considering how increased risk intelligence can add to the business. Considering that consumers now look to the private sector for security, trust is especially important. In fact, "trust" may be consumers' top metric for evaluating and deciding who they want to do business with.

That's why more organizations are aiming for trust by design, an approach that ingrains effective risk management and cybersecurity practices into the texture of the business. Engaging product development teams to instill risk intelligence in decision-making about features and experiences is one example where risk leaders are gaining traction with the business. They will have another opportunity to engage early as automation, cloud services and artificial intelligence are deployed more broadly across the business. Risk managers and cybersecurity leaders should help define the ground rules and guardrails for use of these technologies.

Trust by design enables companies to become digitally confident and more trusted by customers. For risk management teams, it's about providing intelligence and insights to drive growth, increase business value and maintain stakeholder trust. For more on trust by design, click here.

The bottom line: Where cybersecurity is today. Where it needs to be tomorrow.

The rapid pace of disruption brings new risks and threats for financial services firms. The nature and scale of this change encourages information-sharing among firms in areas ranging from engaging the business, to enhancing the content and format of key reports (including those for the board and regulators), to deciding on the right technologies to deploy.

Cybersecurity leaders and teams have a great deal on their plate, but play an essential role in protecting company assets and reputations and an increasingly important one in building trust-based relationships with customers. Cybersecurity reporting, metrics and dashboards, assist organizations in understanding their risk posture, but also help them to make more information decisions as they prepare for the unknown of tomorrow.

Contacts

Jaime Kipnes

Principal, Ernst & Young LLP
Financial Services Organization
+1 212 773 7755
jaime.kahan@ey.com

Mark Watson

Executive Director, Ernst & Young LLP
Financial Services Organization
+1 617 633 5570
mark.watson@ey.com

William Beer

Principal, Ernst & Young LLP
Financial Services Organization
+1 646 306 6290
william.beer@ey.com

Karen Correa

Principal, Ernst & Young LLP
National Advisory
+1 212 773 5255
karen.correa1@ey.com

Sundeep Nehra

Principal, Ernst & Young LLP
Financial Services Organization
+1 212 773 3888
sundeep.nehra@ey.com

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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

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

EY is a leader in serving the global financial services marketplace
Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

US SCORE no. 06111-191US
1903-3083543 BDFSO
ED None

ey.com