Testimony on "Cybersecurity: Risks to Financial Services and Its Preparedness"
Bob Sydow
Principal and Americas Cybersecurity Leader, EY

Committee on Banking, Housing and Urban Affairs
United States Senate
May 24, 2018

I. Introduction

Thank you Chairman Crapo and Ranking Member Brown for inviting me to testify today on behalf of EY. My name is Bob Sydow, and I am a principal at Ernst & Young LLP (EY), which is the US member firm of the global EY network. I lead the EY Americas Cybersecurity practices, have more than 30 years of experience in the cybersecurity field, and have helped build the EY Cyber and Technology practices. Throughout my career, I have worked with Fortune 500 companies on all aspects of information security strategy transformation, cyber risk management, data protection and privacy, identity and access management, cyber threat management and cyber analytics. My current responsibilities include oversight of EY's Cybersecurity practice, which provides assessment and security transformation services across all sectors in the Americas. The EY global network features a Cybersecurity practice spanning 150 countries and more than 7,000 practitioners.

The EY Cybersecurity practice benefits from our unique market position given the work we do within the financial services industry and across all sectors, which make up the modern day cybersecurity ecosystem. Today, I am pleased to testify and address any questions you may have about the state of cybersecurity in the financial services industry, including risks and threats to the sector and economy overall, efforts underway to increase cyber readiness against attacks and what more the public and private sector can do to better protect the economy, companies and, of course, consumers.

We have truly entered a transformative age where businesses are trying to stay one step ahead of the rapid pace of disruption. In doing so, many of our clients look to EY for fundamental end-to-end business transformation strategy and implementation. While transformations can involve everything from supply chain to customer experience, the driving force enabling this change is technology.

However, every new door opened and opportunity presented by innovative technology presents new risks, many of which are cyber in nature. It has never been more difficult for organizations to map and protect the digital environment in which they operate. Digital transformation has created entirely new industries and business models, for example by removing intermediaries in retail shopping and streamlining payment processing. It has triggered the downfall of American corporate giants and created unprecedented connectivity that is nothing short of a revolutionary force, with interdependencies at a scale we've never seen in history.

This is certainly true for the financial services sector, where some of the largest entities can have more than 70,000 third-party vendors connecting into their systems. I can tell you today that the

financial services sector is considered the leader among all others when it comes to adoption of cybersecurity best practices. This is true not only in terms of organization and investment, but also in terms of leading engagement with stakeholders across the ecosystem. The industry is not without challenges, and there is variation among firms. For example, while the largest banks have considerable resources dedicated to cybersecurity risk management, smaller entities often struggle with costs and access to talent. That is not to say these organizations are not committed to cyber risk management or do not take the issue seriously. Cyber breaches and associated losses are not good for business, and when a company's business model depends on customer trust, a cyber event can be even more disastrous.

Trust, after all, is the bedrock of financial services firms and audit firms like EY. Building value successfully by using emerging technologies in the financial services sector demands a thoughtful balance. A focus on preventing cyber threats has, at times, delayed or impacted firms' digital innovation efforts, which can be a challenge in such a highly competitive market. Consumers' rapid adoption of disruptive emerging technology offerings reflects the way financial institutions create solutions that combine transparency, capability and personalization to meet customers' needs on their own terms. At the same time, they are building trust with customers in ways not previously achieved.

Those new solutions come with new threats. Crucially, the many benefits of technology, such as the processing power of the cloud, are also accessible to criminals. Firms that successfully introduce cutting-edge technologies need to infuse cybersecurity risk management practices throughout the entire development life cycle to identify and mitigate new risks as they emerge. This shift in mindset from thinking about cybersecurity as a cost of doing business to seeing it as a growth enabler is not easy, but it is the only viable path forward.

II. Global trends overview

In understanding cyber readiness within the financial services sector, it may be helpful to establish a baseline of comparison. Many US-based businesses, regardless of size, operate globally. As such, it can be helpful to review global cyber trends. For 20 years now, EY has conducted its Global Information Security Survey (GISS) across all sectors to investigate the most important cybersecurity issues facing organizations today.[1] The EY GISS captures the responses of nearly 1,200 participants in 60 countries across more than 20 sectors. Some of the key findings in this year's survey results reflect several of the challenges businesses throughout the economy are struggling to resolve, including with respect to investment, talent and organizational structure. For example:

- 89% of respondents say their cybersecurity function does not fully meet their organization's need
- 75% of respondents rate the maturity of their program to identify new vulnerabilities affecting their technologies as very low to moderate
- 35% describe their data protection policies as ad hoc or nonexistent
- 12% have no breach detection program in place

[1] The 20th EY Global Information Security Survey captures the responses of nearly 1,200 C-suite leaders and information security and IT executives/managers, representing many of the world's largest and most recognized global organizations across 60 countries. The research was conducted between June-September 2017.

- 43% of respondents do not have an agreed upon communications strategy or plan in place in the event of a significant attack
- 57% do not have, or only have, an informal program for gathering intelligence on new threats that could impact the company
- Only 4% of organizations are confident that they have fully considered the information security implications of their current strategy and that their risk landscape incorporates and monitors relevant cyber threats, vulnerabilities and risks

Digital innovation is also transforming the financial services sector — enabling firms to create new products and services, enhance access and experiences for customers, strengthen controls and drive down costs. As banks and other financial services firms define their digital strategies, their operations are becoming ever more integrated into an evolving and, at times, poorly understood cyber ecosystem.

The EY GISS results from banking and capital markets sector respondents, which were significantly weighted toward middle and small market financial services firms (82% of respondents were under $10 million in revenue), also highlight some challenges:[2]

- 85% of respondents say their cybersecurity function does not fully meet their organization's need
- 48% do not have, or only have, an informal threat intelligence program
- 54% of organizations still keep cybersecurity reporting mostly within the IT function
- 12% feel it very likely they would detect a sophisticated cyber attack
- 43% of boards have sufficient cybersecurity knowledge for effective oversight of cyber risks

In a representative comparison, data from the 2017 global EY/Institute of International Finance (IIF) bank risk management survey, which is far more representative of trends at the larger institutional banks, found that cybersecurity has become the number one concern among boards of directors and chief risk officers (CROs) for those institutions:

- 77% of CROs at the largest banks view cyber as their number one risk priority; up 26% from the prior year
- 57% of board directors view cyber as their number one risk priority; up 9% from the prior year[3]

While an individual bank's specific cybersecurity spend is proprietary, the amount of investment by the largest banks is orders of magnitude higher than those downstream, again in large part

[2] 14% of the nearly 1,200 respondents of EY's 20th Global Information Security Survey are from the Banking and Capital Markets sector

[3] "Eighth Annual EY/IIF bank risk management survey, Restore, rationalize and reinvent: a fundamental shift in the way banks manage risk," EY/IIF 2017, https://www.iif.com/system/files/ey_iif_bank_risk_management_survey_2017_restore_rationalize_reinvent_003_13_oct.pdf

because of access to resources. Forbes recently reported that two of the largest banks are spending an estimated $500 million a year each on cybersecurity.[4]

III. Threats and vulnerabilities

Given the prevalence and frequency of attacks throughout the ecosystem and against all organizations, the rapid integration of technological advances is a focus for many of EY's large banking clients. The Global Association of Risk Professionals published a report estimating that attacks and breaches cost businesses $445 billion every year.[5] Data grabs, ransomware attacks, processing disruptions and intentional modification of data can cost a business the trust of their customers, intellectual property and proprietary data. A cyber-related event also has the potential to have a significant effect on an organization's ongoing business operations, reputation, market valuation, financial position, operating results and compliance with laws and regulations.

Attackers may be either indiscriminate or highly targeted, attacking large and small organizations, and are pervasive in both the public and private sector. They are well camouflaged, and exposing attackers requires cybersecurity defenses that identify the threat, even when it adopts the colors of its immediate environment. Against this backdrop, organizations must consider resilience in the context of different categories of threat, which can be broken into three basic threat vectors:

1. Common attacks can be carried out by unsophisticated attackers, exploiting known vulnerabilities by using freely available hacking tools, with little expertise required to be successful.
2. Advanced attacks typically are carried out by sophisticated attackers, exploiting complex and sometimes unknown ("zero-day") vulnerabilities by using sophisticated tools and methodologies.
3. Emerging attacks focus on new attack vectors and vulnerabilities enabled by emerging technologies, typically carried out by more sophisticated attackers performing their own research to identify and exploit vulnerabilities.

Responses must be multilayered and focus on repelling the most common attacks, while also including more nuanced approaches to deal with advanced and emerging threats. As some of these attackers will inevitably breach the organization's defenses, there must also be focus on how quickly they are detected and how effectively breaches are managed.

In terms of common methods of attacks, point of access solutions remain a key element of cybersecurity response and resilience. Tools to help manage these attacks include antivirus software, intruder detection and protection systems, consistent software patch management and encryption technologies that protect the integrity of the data even if an attacker does gain access to it. Employee awareness and cyber hygiene are also crucial to frontline defense, which means changing norms to establish a cyber-minded culture throughout the organization. Of those

[4] "A Lack Of Cybersecurity Funding and Expertise Threatens U.S. Infrastructure," *Forbes*, 23 April 2018, https://www.forbes.com/sites/ellistalton/2018/04/23/the-u-s-governments-lack-of-cybersecurity-expertise-threatens-our-infrastructure/#4803c19149e0

[5] https://www.garp.org/#!/risk-intelligence/all/all/a1Z40000003NYkb

surveyed in the 2017 EY GISS, 68% of financial services respondents considered a careless member of staff as the most likely point of access of the attack.

To defend against advanced attacks, organizations must understand that some attacks will eventually breach their defenses and gain access to the system. As a result, it is critical to plan for and establish controls to identify and contain intrusions as quickly as possible. A Security Operations Center that sits at the heart of an organization's cyber threat detection capability is an excellent starting point and can provide a centralized, structured hub to coordinate all cybersecurity activities. Many such centers are moving beyond passive cybersecurity practices (i.e., waiting for a cyber event to be detected) and focusing on deliberately planned and continuously executed internal campaigns that seek to identify and remove hidden attackers and defeat likely threat scenarios targeting the organization's most critical assets. Even though such approaches have become a leading practice among the largest banks, 65% of financial services respondents to the EY GISS do not have a Security Operations Center — in large part because of resource constraints.

Preparing for and developing responses to combat emerging attacks requires an organization to accept that the nature of some threats will be necessarily unknown. Innovative organizations are imaginative about the nature of potential future threats and are focused on building agility into their cybersecurity approach so they are able to move quickly when the time comes. Organizations with good governance processes underlying their operational approach are able to practice security-by-design, i.e., building systems and processes able to respond to unexpected risks and emerging dangers.

Resource and budget constraints

The incredible pace, not only of technological innovation but also the evolving nature of the threat, necessarily means that there will always be more work than there are resources. While the largest banks have significant budgets dedicated to cybersecurity, many of the regional, midsized and community banks have far more limited resources. Many in the industry are focused on how to best maximize cybersecurity return on investment. At the same time, the latest technology and sophisticated risk management processes are only as effective as the workforce necessary to implement and operationalize them.

As a result, experienced cybersecurity professionals are in exceedingly high demand. The unemployment rate for these individuals is virtually 0%. According to cybersecurityventures.com, there will be an estimated shortfall of 3.5 million professionals in the global information security workforce by 2021.[6] While studies range slightly, a 2017 report estimated a shortfall of 1.8 million unfilled positions in the U.S. cybersecurity workforce by 2022.[7]

As companies continue to identify their needs and capability requirements, the war for talent will only become more acute. Sectors (i.e., financial services and technology) and regions (i.e., east

[6] https://cybersecurityventures.com/jobs/

[7] "2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk," Frost and Sullivan

coast and west coast) that are most attractive to workers are more often able to hire the top talent, which leaves potential gaps elsewhere in the ecosystem.

The cybersecurity environment also demands "life-long learning" through skills developed on the job. It is not enough for a cybersecurity professional to rely on standard classroom experience, conferences, or earning a certification. They must be able to tap into skills acquired over their career. A seasoned, cybersecurity professional is honed over time through on-the-job experiences, exposure to various situations (e.g., incident response), simulations and mentorship.

In reality, cybersecurity capabilities are needed throughout the organization and should not "live" only within the IT function. Truly differentiated cybersecurity professionals understand the business environment in which they operate, are able to convert cybersecurity threats into business implications and then into business strategy/operations. They can translate highly technical jargon into executive-level conversations. This capability is needed in the boardroom, in senior management and across business functions.

Vendors and supply chain management

As noted previously, while the largest companies can afford to build Security Operations Centers, many organizations try to overcome budget constraints by contracting out security functions, such as:

- Threat detection and response
- Vulnerability management (e.g., patching)
- User identity and access management
- Data protection and privacy

Ironically, even though vendors can help provide solutions to some of the resource constraints, third-parties inherently create additional risk. Any single entity can be a potential threat entry point, which may cause a ripple effect across the enterprise or industry. Whereas, traditionally, organizations thought of cybersecurity as a function to protect their own vulnerabilities, they often stopped short of considering the risks to the systems and data that is accessed by the third parties. Heightened regulatory and market focus have continued to put pressure on financial institutions to account for how other companies use and protect their data and manage sustainable operations, especially for critical services.

Because banks are subject to a higher level of regulatory scrutiny, their third-party risk management programs tend to be well established and more mature and robust than other financial services firms. However, as new cyber-related regulations are established and the risk related to these relationships are better understood, other organizations have begun taking steps to mature their programs.

For example, the New York State Department of Financial Services Cybersecurity Regulation required financial services firms to implement rigorous third-party cybersecurity risk management policies and procedures across the full life cycle of the relationship with third parties based upon the third parties risks to the organization..[8] The European Union's (EU)

[8] EY's *Overview of the finalized Cybersecurity Requirements from the New York State Department of Financial Services (DFS)*, EYGM Limited, February 2017

General Data Protection Regulation (GDPR) puts the onus of specific privacy requirements in the hands of the organizations and their third-party vendors collecting, storing and processing personal data. Firms subject to the GDPR will have to demonstrate their compliance with the requirements by May 25, 2018. The GDPR includes incredibly challenging requirements, such as the right to be forgotten, data portability, 72-hour breach notification, data privacy impact assessments and privacy by design. While this is being driven abroad, it significantly affects US companies offering goods or services to EU residents or those with an establishment in the EU.[9]

IV. Cyber risk governance

The board's role in fostering a cyber minded culture

At EY, we have found that directors serving on financial services boards receive a steady stream of news about cyber attacks, and most have received multiple briefings from their executive teams if not by federal national security officials. The primary challenge that directors and their firms grapple with is how to keep pace with fast-changing cyber risks in terms of the vulnerabilities or the new sources of risk that they create. Keeping up with known threats and vulnerabilities is difficult enough, but the scope of unknown cyber risks seems much larger than other, more traditional risk domains.

Directors appreciate that cyber attacks and breaches carry potential material risks and may now go beyond a profit motive to one associated with destroying data, manipulating systems and/or data, or incapacitating systems. A 2018 Council of Economic Advisors report highlighted that, of more than 1,900 breaches reported in 2016, almost 25% of breaches were in the financial services industry.[10] Hence, from a risk perspective, financial services boards understand both the potential impact and probability of cyber attacks are on the rise. EY has found that the most effective boards are implementing more robust cyber risk governance in five ways:

1. *Establishing and assessing cyber risk management maturity:* Boards need to understand the maturity of their organizations' approach relative to evolving industry and regulatory trends. Focusing on the chief information security officer's (CISO's) organization is necessary but no longer sufficient on its own. A cyber risk maturity assessment should be broad in nature, considering people, process and technology as well as existing and planned improvement or remediation activities. Foundational elements need to be in place, such as a firm-wide, consistent view of what constitutes cyber risk and the current vulnerabilities and threats. In that context, the effectiveness of existing controls can be evaluated.

2. *Measuring and evaluating cyber risk:* The view on program maturity needs to be combined with a proper assessment of existing threats and vulnerabilities and the evolving threat landscape. Boards should press management to quantify cyber risk as much as possible so that quantitative statements on the degree of cyber risk are

[9] See EY's *GDPR: demanding new privacy rights and obligations* in the Appendix or visit http://www.ey.com/gl/en/services/advisory/ey-general-data-protection-regulation

[10] *The Cost of Malicious Cyber Activity to the U.S. Economy* (page 19); The Council of Economic Advisors, February 2018.

incorporated into the firm's risk appetite statement.[11] The cyber risk appetite statement should link directly to cyber and technology operational thresholds and tolerances.

3. *Developing more robust and transparent management reporting on cyber risk:* Boards should insist on more credible cyber risk reporting, in the context of the approved cyber risk appetite. Boards should also determine how they evaluate the quality, accuracy and timeliness of cyber metrics. Too often, firms use key performance indicators for technology as proxies for real cyber risk reporting. Also, cyber loss estimates are usually too narrow, focusing on cost of recovery and fixing identified problems rather than the broader opportunity costs (e.g., lost business or customers) from technology problems created by cyber attacks. In EY's view, a more expansive view of cyber losses would materially improve decisions made around cyber investments. Cyber metrics should align with the broader firm risk taxonomy and align with metrics for operational, technology and privacy risk. Over time, cyber metrics should become more discrete and evolve to be more forward-looking.

4. *Apportioning oversight duties across the board and committees:* Boards should challenge how they oversee cyber risk across their own governance structure. Certain aspects of cyber risk management could fall to the full board or across various committees; for example:
   - The full board of directors might discuss the integrated, enterprise-wide cybersecurity strategy, supported by regular cybersecurity briefings on the evolving threat environment so every director is informed on the effectiveness of the cyber risk management program.
   - The audit committee often oversees how internal audit and compliance are evolving their reviews and oversight of cyber risk and regulations. The audit committee also oversees the work of the external auditor and may review the privacy dimensions of cybersecurity.
   - The risk management committee may engage the CRO on the evolution of the cyber risk strategy, including the cyber risk appetite and cyber risk metrics and reporting.
   - The operations and technology committee may engage the CISO, chief information officer (CIO), and chief technology officer (CTO) on the overall front-line cyber strategy, security operations, threat intelligence and incident response, as well as approaches to incorporating cybersecurity into innovation, digital and FinTech strategies. (To the extent such a committee does not exist, these dialogues would typically span the audit and risk committees.)
   - Personnel and compensation committees might engage the chief human resource officer on cybersecurity talent acquisition, retention, training and awareness strategies.
   - Nominations, governance and public affairs committee may evaluate cybersecurity and technology expertise among the board of directors, the board's ability to access internal or external cyber expertise, and how to effectively communicate with shareholders.

[11] For an example of an effective cyber risk dashboard, see Appendix F of the "Cyber-Risk Oversight: Director's Handbook Series," National Association of Corporate Directors, 2017.

5. *Overhauling cyber training for directors*: The board should revisit its strategy for keeping directors abreast of cyber threats, trends and the evolving business implications. EY has found that too often, this equates to annual presentations by the CISO but far more is needed. Aspects of cyber risk management should be built into an ongoing training program throughout the year, with overview sessions and deep dives on the most relevant topics and issues.

Ultimately, the board is accountable for ensuring that management adapts quickly enough to manage this enterprise risk more effectively and efficiently, and it is charged with providing a credible challenge to management's approach.

At EY, we believe that boards must be educated about cybersecurity so they are able to make appropriate decisions anchored in sound logic and data. They should embrace the challenge of mastering knowledge in this new, emerging area. By doing so, boards will not only be protecting shareholders but they will be enhancing the company's value. Directors should also set the tone at the top and concretely demonstrate that cybersecurity is an enterprise-wide priority and not just one that sits within IT. Board members possess both formal and informal responsibilities, as well as a duty to instill management accountability to drive outcomes, including with respect to cyber talent strategies, pressing management to identify high value assets, and incorporating cybersecurity into an organization's risk appetite statement.

The board should also elevate the position of an organization's cybersecurity leaders. For example, a leading practice is for the CISO to report directly to the C-suite, most commonly the chief operating officer (COO), chief administrative officer (CAO) or CIO. Consideration should also be given to embedding cybersecurity leaders throughout an organization, and the CISO should be well-versed in business strategy so that she or he can link the cybersecurity threat posture and risk tolerance to business drivers and protect high value assets. To make cyber strategy even more relevant, the board should anchor it to already existing risk frameworks that the organization employs, like those in finance, operations and procurement, in order to safeguard its reputation.

Cyber risk management across the three lines of defense[12]

Many companies seeking to establish an effective enterprise risk management system adopt a governance structure referred to as the three lines of defense (3LoD), which is common among financial services firms. The first line operates the business, owns the risk, and designs and implements operations. The second line defines policy statements and the risk management framework, provides a credible challenge to the first line, and is responsible for evaluating risk exposure for executive management and the board to consider when establishing a risk appetite. The third line of defense, which is also commonly referred to as internal audit, is responsible for the independent evaluation of the first and second lines.

EY has found that establishing a 3LoD approach to cyber risks is not a trivial task for an organization, but it is essential in the cyber-world we have entered. Financial services firms are still grappling with how to best implement the model across their businesses for existing non-

[12] This includes excerpts from *EY Cyber risk management across the three lines of defense*, EYGM Limited, April 2017.

financial risks. Adding cyber risk management as well as strong board oversight during the implementation of the three 3LoD model poses an even greater challenge for organizations.

First line of defense

A strong first line of cybersecurity defense requires a significant effort. Whether in the retail bank, investment bank, corporate bank, private bank or any other area, business heads will have to perform a thorough examination to determine whether the business is doing enough to manage cyber risk. Information security groups can no longer apply one-size-fits-all solutions to the entire enterprise. Instead, each line of business must carefully define the cyber risks and exposures it faces. Cyber risks need be woven into the fabric of the first line's risk and control self-assessment and into fraud, crisis management and resiliency processes.

EY teams advise organizations to achieve a better understanding about the interrelationship between their activities and cyber risks. The lines of business will need to actively monitor existing and future exposures, vulnerabilities, threats and risks associated with their activities. In addition to leveraging technologies, businesses need to determine the impact that cyber risk will have on its clients, operational processes and strategies. These new responsibilities require significant investment in people and tools, including upgraded monitoring and analytic capabilities to provide improved assessments of current levels of cyber risk.

Second line of defense

The independent second-line cyber risk management function manages the enterprise cyber risk appetite and risk management framework within the context of the overall enterprise risk strategy. This group challenges the first line's application of the board-approved cyber framework and appetite. Second-line risk management plays a critical role in managing cyber risks and should not be walled off as a separate risk function. As the keeper of a firm's board-approved risk tolerance, it determines how to appropriately measure cyber risks, embedding quantitative and qualitative (e.g., reputational) thresholds for cyber risks into the statement of risk tolerance for the firm. Moreover, these clearly established appetite and associated thresholds need to cascade down into the operations for each line of business.

Given the relative novelty of applying the 3LoD model to cyber risk, most of the first and second lines focus appropriately on more effective management of these risks rather than the narrower issue of compliance. However, with an increasing volume of regulatory guidance and mandatory requirements stemming from industry, professional and regulatory standards, cyber will increasingly constitute a material compliance risk. Accordingly, it is EY's view that financial institutions should integrate cyber risk compliance into second-line risk management.

Third line of defense

Traditionally, the main role of the third line of defense has been to provide an independent and objective assessment of the firm's process across the first and second lines of defense, with the focus on operational effectiveness and efficiency as part of the firm's overall risk governance approach. Regulators are now focusing on how effective and independent a firm's internal audit team is when it comes to reviewing the firm's approach to cybersecurity. For example, banking regulations focused on cybersecurity often include references to the importance of an "annual independent assessment," such as those included in Federal Financial Institutions Exam Council

(FFIEC) and National Institute of Standards and Technology (NIST) requirements and guidelines.

As a foundation, EY recommends that the internal audit team include within its overall audit plan an evaluation of the design and operating effectiveness of cyber risk management across the first and second lines of defense. Traditionally, industry standards, such as the NIST's Cybersecurity Framework guidelines have been used as the benchmark for evaluating a firm's effectiveness. Going forward, internal audit teams at financial institutions may need to create their own framework or apply multiple industry frameworks. By doing so, internal auditors will maintain greater independence in assessing cyber risk management effectiveness, eliminating the potential blind spots that can result from using a common standard throughout all three lines of defense.

Under the 3LoD model, internal auditors perform procedures such as assessments, validation of applications and technology infrastructure, evaluations of third-party risks, conduct independent penetration testing and vulnerability assessments, incorporate cyber into regular audits, and have a responsibility to stay abreast of cyber threat intelligence.

Getting the cyber 3LoD right

Regulators are encouraging utilization of the 3LoD model to compel banks to improve their risk management in response to failures in recent years. Firms have successfully implemented the 3LoD model in the area of financial risks, such as credit and liquidity. However, there are challenges in areas of non-financial risks, including cyber risk. Getting this right will take time. Given system-wide cyber risks, EY believes the financial services sector needs to move quickly to get the fundamentals in place so that, together, individual firms and the industry as a whole become better protected, more resilient and capable of responding quickly and effectively to the inevitable and increasingly potent attacks the industry will experience over the coming years.

The three lines of defense support cyber resiliency in financial services[13]

Today, the financial services industry is facing tougher questions from external parties as to their cyber resiliency strategy. Increasingly, regulators, investors and major clients are demanding evidence that firms' cyber resiliency strategies are effective. Stakeholders want to know how the organization is reducing the likelihood of a disruption to services; how it will manage prolonged systems outages, including how transactions will be processed; and how it will recover effectively in a timely and well-controlled manner. Financial services firms recognize that cyber resiliency relates to the seamless maintenance and ongoing delivery of operations during a disruption. This includes how firms govern and challenge cyber resiliency with the 3LoD. Additionally, the industry is working on advancing reduction in risk in the financial ecosystem through initiatives led by private sector industry organizations in collaboration with government agencies and the intelligence community. EY recommends that key areas of resiliency include:

1. *Risk-assess cyber resiliency*
   Firms should assess their cyber risk profile and identify major risks, threats and vulnerabilities. This requires:

[13] This includes excerpts from *EY Cyber resiliency: evidencing a well-thought-out strategy*, EYGM, August 2017.

- An effective risk assessment process, which includes taking an end-to-end view so that the entirety of the process and supporting systems, vendors and dependencies can be identified.
- Building effective controls to reduce residual risks to levels within the firm's overall risk appetite for resiliency. This includes understanding how dependency on third parties impacts the control environment.
- An enterprise-wide, prioritized view on critical processes and flows**.** Given finite resources — management time, budget and people — firms inevitably have to prioritize certain resiliency activities. There will likely be differing views within each firm about what constitutes criticality.

2. *Identify, architect and protect systems, especially those most critical to the firm and the broader financial services ecosystem*
   High value assets that are "sector-critical systems" are generally easier to identify, e.g., the key intraday settlement and clearing systems that help the financial system operate smoothly. Beyond those systems and assets, however, differing views will exist as to what is critical. Once identified, EY advises firms to:
   - Identify those individual systems or assets' ecosystem.
   - Evaluate and, where necessary, improve system architecture and design. Critical systems have to be sufficiently flexible, agile and resilient.
   - Evaluate if systems and tools used to monitor infrastructure present major vulnerabilities themselves. After all, if these tools are breached, attackers could gain access to an even broader swath of important systems.
   - Evaluate system obsolescence**.** Every firm has adopted its own strategy that may take into consideration the pace at which new versions of software or hardware are installed, the approach to patching, and the degree to which the firm will depend (or not) on systems that are no longer vendor-supported. It is important that firms carefully consider if a differentiated strategy is needed for critical systems. As recent global ransomware attacks have shown, system outages can be traced to dependencies on old versions and bad patching practices.

3. *Manage critical third parties and other key dependencies, especially those that support or connect with critical processes and systems*
   An enterprise-view of critical vendors should be evaluated regularly in the context of recovery and resolution planning. Organizations should evaluate or re-evaluate vendors' resiliency and cybersecurity practices, build contracts that include terms addressing performance and key risk indicators, and establish a process to regularly provide real- or near-time monitoring of critical vendors. Many recent breaches highlight how even vendors outside of the financial ecosystem can create vulnerabilities if systems are not properly segmented.

4. *Detect, respond, recover and communicate*
   Even the most sophisticated organizations will eventually experience a cyber breach. EY advises firms to have fully developed response plans in place before an event occurs. All corporate officers and functions — from the board, executive management, risk functions and general counsel to business units and information technology — need to be considered in

incident remediation. Many incident investigations are far more complicated than simply removing malware. They often involve reviews of the technical facts combined with operational, legal and financial impacts. As a result, victim organizations often call in multiple forensic investigators and counsel to address the variety of external inquiries.

5. *Test systems and recovery plans*
   EY advises financial services firms to regularly test cyber resiliency strategies. The first line has to test the effectiveness of its own controls, in the context of its risk assessment. The second and third lines should review some of these processes to validate the first line:
   - "Tabletop exercises" or role-playing scenarios are an important way to test plans, educate participants and identify areas for improvement. Scenarios should be realistic, include participants from across the 3LoD, and include specific cyber scenarios.
   - Each of the 3LoD should conduct routine tests to assess the degree to which systems can be penetrated. This typically requires external third-party support.
   - In addition to tabletops, when possible, firms should participate in "war games" that involve stakeholders from across the industry. These exercises help firms better appreciate scenarios that could impact the entire financial sector. War games also help organizations better manage expectations about how the market or peers will react.
   - In the end, testing, tabletops and war games are only helpful if identified deficiencies are addressed.

Resiliency extends beyond cyber attacks

At EY, we believe that achieving cyber resiliency requires an integrated approach across technology and the front-line businesses, cybersecurity and information security, the three lines of defense, and across the entire organization, including the board of directors. In practice, resiliency is a broad-based concern that firms can only address effectively and efficiently by integrating a set of disparate activities across the enterprise. That is true for operational resiliency, as much as it is for cyber resiliency.

V. Leveraging cybersecurity advances to fight financial crimes

Financial institutions' customers, whether individual consumers or commercial business partners, expect an experience that is consistent, positive and frictionless. To support digitized banking experiences, financial services providers increasingly rely on cloud-based off-premise solutions in conjunction with their on-premise legacy applications and infrastructure, as well as upon the integration of many third-party technologies, both open and closed source. At EY, we have observed a blurring of the lines between financial services, FinTech, and technology companies. This will only continue to progress as more innovation and efficiency is introduced into digitized and integrated services.

Each step up the integrated chain of financial services brings risks and challenges for fraud and authentication, as well as the confidentiality and integrity of transactions. Financial services firms have responded to consumer expectations by adding more digital and traditional banking channels and increasing security as channels become more virtual. Complex cross-channel attacks that combine information gathered from social media as well as digital and traditional banking channels are on the rise. Similar to fraud scenarios, anti-money laundering (AML) activities can use similar channels, though in a much less complicated way. As a result,

cybersecurity vulnerabilities are increasingly being identified as the "root cause" of fraud events. Advanced technologies and the commoditization of cyber tools, tactics and procedures allow criminals to attempt fraud at unprecedented scales.

There are many challenges, including protecting and monitoring customer touch points across various channels. EY has found that attacks are increasingly targeting data itself as the asset of value. Information sharing between cybersecurity and fraud programs may be missing, insufficient, ineffective or difficult to act upon. A number of corporate cultures do not recognize the link between fraud and cybercrime; although, more firms are drawing links and looking to integrate these capabilities. EY has found that criminals take advantage of organizational issues, and functional silos that exist at many organizations that can make it easier for fraud to be committed in ways that are difficult to detect.

In addition, ransomware attacks, designed to be destructive or to obscure application data, are increasingly common. Ransomware attacks are a very serious concern given that they can result in interruption, disruption or destruction of critical business services. As digitization accelerates, many businesses have lost their ability to protect their enterprise, and they have also lost their capability to understand their infrastructure. As such, there exists a concerning risk intersection between cyber and business resilience.

VI. AICPA's Cybersecurity Risk Management Reporting Framework

Another major challenge in the market is how to communicate effectively with internal and external stakeholders about a company's cybersecurity risk management activities. Limited options have been available to provide relevant, validated information that enable various stakeholders to make informed decisions. Investors trust the board to oversee the management of cybersecurity risk. Boards trust management to effectively manage cyber risk, and often management relies upon various third-party vendors to help support cyber efforts.

However, there has been no independent, validated basis to warrant such trust. To help address this market need, the American Institute of Certified Public Accountants (AICPA) recently undertook an effort that built upon the accounting profession's historical role of promoting trust and confidence in the market. In 2017, the AICPA issued an evaluation framework with an optional reporting model that can provide stakeholders with: (1) transparency into key aspects of an organization's cybersecurity risk management program, (2) confidence in the adequacy of the program and (3) assurance as to the program's effectiveness.

The framework that the AICPA developed is different from existing "implementation frameworks" developed by NIST, International Organization for Standardization (ISO) and others. Implementation frameworks lay out the key building blocks that should be included in a risk management program. The AICPA's evaluation framework, on the other hand, focuses on the outcome of the risk management program and whether a program is properly designed and verified to be operating effectively. The distinction is subtle, but significant. Ernst & Young LLP supports the AICPA guidance, which is voluntary in its application and enables companies to communicate with its stakeholders on three levels:

- At the entity-level, where an organization could report on the effectiveness of its overall cybersecurity risk management program to board members, investors and others.

- At the service provider-level, where an organization could report on the effectiveness of key aspects of its cybersecurity risk management program relative to an outsourced service that they provide to the market.
- At the supply chain-level, where an organization could report on the effectiveness of its processes and key aspects of its cybersecurity risk management program relative to the manufacturing and distribution of supply chain goods provided to the market. This component of evaluation framework is still in development, and final guidance will be available in early 2019.

We at EY note that such attestation engagements cannot ensure a company will be free from material cybersecurity events, but evaluation frameworks enhance the level and quality of communication taking place between companies and their stakeholders to a point where more effective risk management decisions can be made. They can enhance stakeholder confidence in the cyber management security program being employed. The receipt of an unqualified opinion on an attestation engagement is intended to convey that the entity has implemented reasonable controls to complicate attackers' efforts and to detect, respond and recover from a cybersecurity event: (1) when measured against criteria that have been vetted in the marketplace and deemed to be suitable for the intended purpose and (2) based on specific cybersecurity objectives that the company is obligated to achieve. The stakeholder in this case can be the board, or, if the board chooses, it could be reporting to the public in some manner.

In addition to being more comprehensive and business-centric, if a report under one of the AICPA's cyber-related reporting options is issued, adherence to the evaluation framework will be essential, as the criteria and areas of focus will generally serve as the basis of those engagements. Ernst & Young LLP believes the voluntary use of the AICPA guidance can help boards, management, investors or analysts gain a more complete, objective understanding of an organization's cybersecurity risk exposure and controls. It may also be a way for companies to differentiate themselves in the market and reassure customers, investors and other stakeholders.

VII. Role of policymakers

EY is committed to building a better working world and commends the Senate Banking Committee for convening this hearing to engage in meaningful dialogue on this systemic issue. Understanding the nature of cyber risk is the first step in developing more effective solutions. Every organization, public or private, faces this challenge and is exposed to the threat. Engaging your colleagues in Congress on this topic, pursuing and facilitating systems modernization and better cyber risk management in federal, state and local governments, and encouraging the American people to improve their own understanding of cyber challenges and vulnerabilities are important steps this committee can take. Focusing on long-term policy solutions to develop and increase the cyber workforce and working to resolve sector and resource issues known to exist are other opportunities for policymakers to address these challenges.

Unfortunately, there is no silver bullet — no single legislative, regulatory or market solution — that can solve this challenge. And the challenges are great. Not only do threats evolve day-by-day, but those who want to do harm are not constrained by regulatory, liability or jurisdictional issues, let alone ethics. Policymakers and the business community must work together to

improve cyber information sharing and develop collaborative, flexible and harmonized policy solutions that help organizations better respond to the dynamic nature of the challenge.

While no one can guarantee that any or all attacks can be prevented, the market is developing best practices and ways to mitigate risk and impact. Companies that exercise good faith efforts, establish cyber risk management frameworks and adopt such best practices as outlined in this testimony should benefit, not only within the company, but in the eyes of stakeholders, regulators and enforcement agencies, especially relative to liability and penalty measures. Given this committee's experience and expertise in the area of corporate governance, and acknowledging the sector and resource constraints that all organizations and this nation face, investigating ways to incentivize responsible and effective corporate governance and risk management strategies by rewarding good behavior could be an area for the committee to pursue.

Given its role in the ecosystem, I would also encourage Congress to consider the modernization and improvement of the cybersecurity posture of all branches of government as well. The same approach to comprehensive enterprise-wide cybersecurity assessments being pursued in the private sector are equally relevant to the public sector. Holistic cybersecurity assessments should be conducted on a regular basis and should span a public sector organization's overall risk management structure. This would help give executive leadership and the American people the confidence that their single most important mission asset — information — is sufficiently protected against current and future threats.

Just as no government agency wants to be hacked, no company wants to be hacked. There are many organizations across the ecosystem that should be commended for their efforts to manage and mitigate cyber risks. The financial services sector may have its challenges, but it is the gold standard in the market today. EY is working with our financial services clients and companies from all sectors to be responsive to the many cybersecurity challenges we all face. While EY does not have the solution to this systemic challenge, we are doing our part to build a better working world by helping our clients develop and implement better risk management controls, educating boards and senior management, and developing a number of market-based solutions to better manage cyber risk and resource shortage challenges. The AICPA's cybersecurity evaluation and reporting framework is an example of a voluntary, market-based solution that can help boards, shareholders and senior management alike.

* * * * * *

I thank the committee for granting me the opportunity to testify today and would be happy to take any questions.

Appendix

Building a better working world

GDPR: demanding new privacy rights and obligations

Perspectives for non-EU financial services firms

In the race to compete in today's digital world, organizations are using social, mobile, big data, analytics and the Internet of Things to gather as much information on their customers as possible, while simultaneously trying to do everything possible to protect their organizations from cyber risks that come from the outside and within. In this environment, privacy protection can become an afterthought, bolted on to information security programs in an ad hoc manner or, in the worst case, organizations have elected to ignore the issue.

For years, regulators and privacy commissions around the world have attempted to regulate privacy protection and develop privacy standards, such as privacy by design (PbD), for organizations to adhere and adopt. However, even as regulators pushed accountability, many organizations saw it as more voluntary than mandatory. They were content to address the letter of the law outlined in the legislation as opposed to its spirit, i.e., to meet minimal compliance obligations without taking responsibility for their role in protecting their customers' or employees' information.

With the forthcoming implementation of the European Union's (EU) General Data Protection Regulation (GDPR), and its implications for organizations across the globe, the days of organizations leaving the responsibility for privacy protection to someone else are about to end. The EU's GDPR puts the onus of specific privacy requirements in the hands of the entities collecting, storing, analyzing and managing personally identifiable information.

Firms subject to the GDPR will have to demonstrate their compliance with the requirements by May 25, 2018. The GDPR is much more demanding, and applies more broadly, than existing EU data protection requirements. Each requirement by itself – such as the right to be forgotten, data portability, 72-hour breach notification, data privacy impact assessments and privacy by design – is demanding, but in aggregate, the GDPR is very onerous.

For more cyber and privacy insights, visit ey.com/fsGDPR **or** ey.com/fscyber

Note: The General Data Protection Regulation is European Union regulation 2016/679, made 27 April 2016, implementation date 25 May 2018.

To date, many non-EU financial services firms have been slow to react to the GDPR. While some firms have taken a proactive and comprehensive approach, many have not. Even firms in the EU are delayed. For example, a recent UK government survey highlighted that only 6% of the Financial Times Stock Exchange (FTSE) 350 companies report being completely prepared to meet the GDPR compliance requirements.[1]

Firms need to focus on the GDPR now. Time is running out!

Immediate next steps

- Educate key stakeholders, including the board of directors
- Risk-assess (including legal applicability) whether the GDPR applies to your organization
- Establish cross-function and cross-business governance structure for assessment of the GDPR's applicability to business operations, evaluation of readiness and management of your overall GDPR remediation efforts
- Conduct a privacy impact assessment, with a strong focus on high-risk data flows of business processes
- Conduct a GDPR gap assessment, with a particular focus on governance, policies, technology, external dependencies (e.g., vendors), existing data flows ("high-risk") and processing operations
- Design and execute a prioritized implementation plan to address gaps based upon risk tolerance, risk priority, resourcing and investment

[1] "FTSE Cyber Governance Health Check Report 2017," HM Government, Crown copyright 2017.

What is the GDPR?

The GDPR is an omnibus data protection law that builds upon, expands and ultimately replaces the EU Data Protection Directive. The GDPR gives individuals new rights over their data, which heightens the accountability on entities collecting, storing, analyzing and managing personally identifiable information. This covers any information relating to an identified or identifiable natural person, such as name, identification number, location data or one of more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity on the nature of the person, as well as online identifiers (e.g., IP addresses). A data subject can be a customer, employee, contractor or third party. Released in 2016, and due to come into effect May 25, 2018, the GDPR applies to any organization, regardless of geographic location, that controls or processes the data of an EU resident in a proscribed way. It dictates to what extent personal data may be collected, the need for explicit consent to gather such data, requirements to disclose breaches of data and stronger powers to substantially fine organizations that fail to protect the data for which they are responsible. And it has real teeth.

The GDPR prescribes certain responsibilities and liabilities to controllers and processors of personal data. It is important to understand these terms as they are defined within the GDPR.

- **Controller:** a body (alone or jointly with others) that determines the purposes and means of the processing of personal data
- **Processor:** a body that processes personal data on behalf of the controller; processing activity can include collecting, organizing, storing, disclosing, using, etc.
- **Personal data:** any information (single or multiple data points) relating to an identified or identifiable natural person such as name, employee identification number or location data

The GDPR imposes new obligations on both controllers and processors of personal data, emphasizing accountability and requiring greater documentation and records.

Firms have until May 25, 2018, to implement changes and comply with the obligations of the GDPR. Penalties for failing to comply with the GDPR's basic processing principles may subject the organization to fines up to €20 million or 4% of the organization's total global revenue, whichever is greater.[2]

Key facts about the GDPR

Applicability: applies to entities – including third parties that are (i) established in the EU, (ii) providing goods or services to EU residents or (iii) are monitoring the behavior of individuals in the EU

Fines: up to €20 million or 4% of the organization's total global revenue, whichever is greater; also provides individuals new rights to bring class actions against data controllers or processors, if represented by not-for-profit organizations, which heightens litigation risk

[2] EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

GDPR highlights

Organizations will have only 72 hours to report data breaches.

Privacy-by-design principles must be incorporated into the development of new processes and technologies.

Explicit and affirmative consent will be required before processing personal data.

Most organizations will need to designate a Data Protection Officer.

Organizations will have to maintain records of processing activities.

Organizations will need to scale security measures based on privacy risks.

International transfers are prohibited except through certain mechanisms.

Organizations will report to one supervisory authority.

Organizations will have to facilitate customers' and employees' right to erasure (of data), right to portability, and an increased right of access.

GDPR impacts

Penalties for failing to comply with the basic processing principles of GDPR may subject the organization to fines up to

€20 million or **4%**

of the organization's total global revenue, whichever is greater.

Organizations have only until

25 May 2018

to implement changes and comply with GDPR obligations.

Imposes new

obligations

for both controllers and processors of personal data

Places a greater emphasis on

accountability

requiring greater

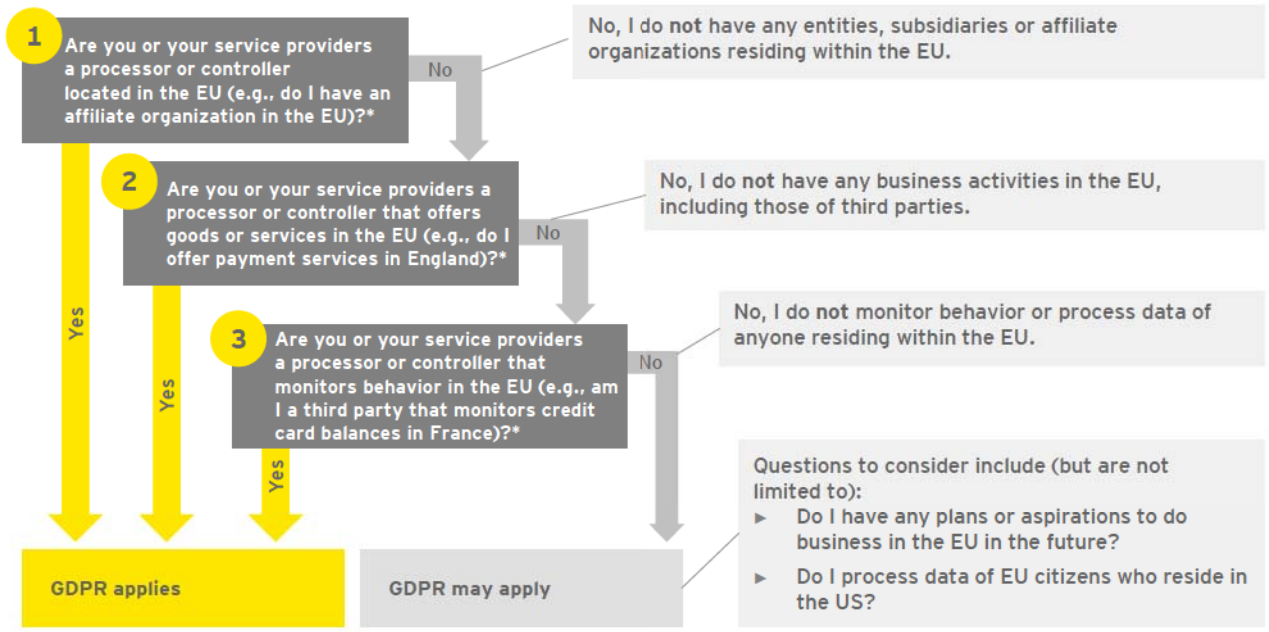
documentation

and records

Is the GDPR applicable to you?

Many non-EU financial services firms have determined that the GDPR doesn't apply to them with limited understanding of how the regulation actually works. Figure 1 outlines three distinct questions that can be used to assess applicability.

Figure 1: Three key questions to assessment applicability



*Note - the responses to these questions should be evaluated based on the facts and circumstances in your organization and discussed with legal counsel.

The question, "Are you or your service providers a processor or controller that monitors behavior in the EU?" captures a broader range of activities than many firms think. Consider centralized functions that conduct surveillance, such as for fraud, anti-money laundering, sanctions or cyber threats. To the extent those functions use data related to EU residents, your organization may be subject to the GDPR requirements. Similarly, many firms' websites continuously monitor traffic and users, and some leverage third-party vendors in the website execution. Those activities – of the firm or the third parties – may subject your organization to GDPR requirements.

Firms are advised to consider these questions and discuss them with their legal counsel. However, firms may be inclined to take too much of a legalistic approach to the GDPR, depending too heavily on outside counsel's advice on whether or how the GDPR applies to their firm. In addition to the legal input, firms should undertake a risk-based assessment to evaluate the relevance and applicability of the GDPR based on a fact-based, documented review of the degree to which their operations or third parties access, store or monitor data related to EU residents. Such an approach takes into the account the firm's strategy, growth plans, risk tolerance, existing controls and capabilities, as well as other contextual factors that may impact the determination of applicability.

What are the main GDPR concepts and requirements?

The GDPR enhances the data protection rights of EU data subjects. In general, firms will need to provide easier access to personal data, with clear and understandable information on its processing, use and storage.

Major requirements and concepts include:

- **Data protection impact assessment (DPIA):** DPIAs (also known as a privacy impact assessment or PIA) are required for all process operations of an organization. DPIAs should be viewed as tools that can help organizations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. There is a debate in the marketplace about the required approach: are data flows required for GDPR or can data narratives be utilized? Generally, firms seem to be completing data flows to properly assess the GDPR, especially to understand data flows in their high-risk processing activities. An effective DPIA will allow organizations to identify and fix problems, reducing the associated costs and damage to reputation that might otherwise occur.
- **Data privacy accountabilities:** the GDPR attempts to define what privacy accountability means in practice through requirements around proactive monitoring and personal data records. The GDPR states that the controller is responsible for confirming that all of the GDPR privacy principles are adhered to and that firms can demonstrate compliance. Each organization has to understand the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation and integrity and confidentiality. The DPIAs will help in this regard.
- **Condition for processing:** the processing of personal data is only lawful if it is permitted by the GDPR and has proper customer consent. If the controller does not have a legitimate reason for a given data processing activity, then that activity is not allowed – firms must have at least one legitimate reason for processing, which can include the individual's consent, contractual necessity, legal obligation, regulatory requirements or public interests.
- **Data protection officer (DPO):** firms that establish they conduct large-scale systematic monitoring of EU residents' data or process large amounts of sensitive personal information have to appoint a DPO. "Large-scale" could be as small as the processing of data on more than 5,000 subjects in any 12-month period.[3] DPOs have significant accountability for adherence to the GDPR requirements, and they must be appropriately qualified in data protection laws and practices, independent of management,have access to the necessary resources to monitor GDPR compliance and be actively included on all relevant data protection discussions and decisions. The regulation calls for the DPO to report to the "highest management level," which EU guidance suggests could be the board of directors.[4]
- **Privacy by design (PbD):** is the practice of establishing and implementing privacy controls and principles into business processes and systems as they are being developed and built, rather than layering on controls after deployment. Although PbD has been championed for years by privacy commissions around the world as a leading privacy standard, in our 2015 Global Information Security Survey, only 18% of survey respondents indicate that they have applied PbD to their new processes and technologies.[5] Under the GDPR, organizations will now be required to design policies, procedures and systems that follow PbD principles at the outset of every product or process development.
- **Right to erasure:** the right to erasure enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This right creates significant data retention challenges for firms. The broader EU principle this relates to is the right to be forgotten, whereby residents have the right to have personal data on public media deleted (including by third parties).

[3] "Top 5 Priorities to Prepare for EU GDPR," *Gartner website*, www.gartner.com/smarterwithgartner/top-five-priorities-to-prepare-for-eu-gdpr, 20 June 2017.

[4] Article 29 Data Protection Working Party, Guidance on Data Protection Officers (DPOs), April 5, 2017.

[5] *Can privacy really be protected anymore? Privacy trends 2016*, EYGM Limited, 2016.

- **Individuals have the right to have personal data erased and to prevent further processing:** under the following circumstances:
  - Personal data is no longer necessary in relation to the purpose for which it was originally collected/ processed.
  - Individual withdraws consent.
  - Individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
  - Personal data was unlawfully processed.
  - Personal data has to be erased in order to comply with a legal obligation.
  - Personal data is processed in relation to the offer of services to a child.
- **Consent and notifications:** under the GDPR, consent must be freely given, specific, informed and unambiguous, indicating the data subject's agreement to the processing of personal data relating to him or her. It should be noted that consent is not required if there is another basis for use – in practice, most firms will point to a signed contract as their basis.

  Breach notifications under the GDPR must be done within 72 hours of the organization becoming aware of the breach. If the breach is sufficiently serious to warrant notification to the individual data subject, the organization responsible must do so without undue delay. Failing to notify or noncompliance can result in a significant fine up to €10 million or 2% of global revenue.[6] Many practitioners expect that when the EU issues new guidance later in 2017 on the breach requirements, it will recognize that it will often be impossible to investigate a breach fully within that time period and will allow firms to provide information in phases, so long as the relevant data protection authority, or DPA, is notified.
- **Data portability:** the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. The provision allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. It is the responsibility of the controller to confirm this capability exists.

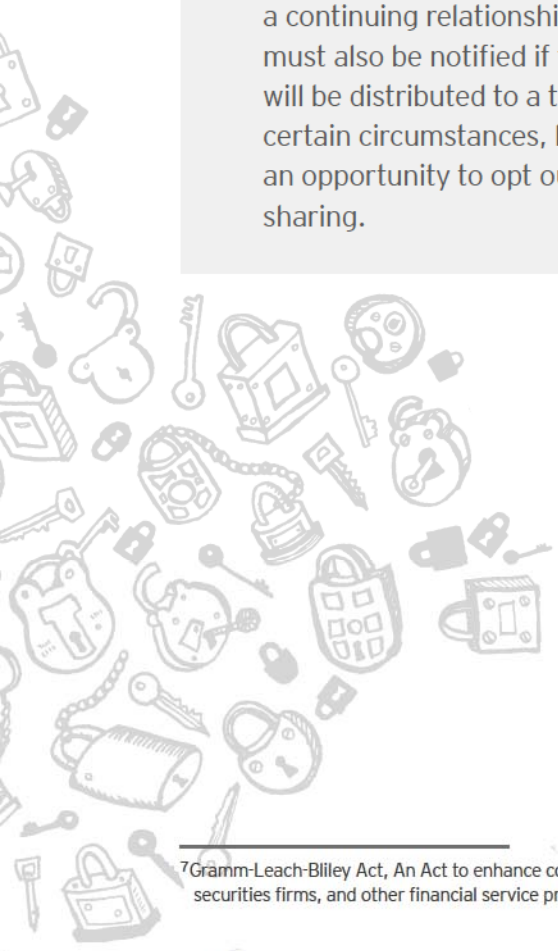
[6] EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

What is the difference between EU GDPR and US GLBA?

The focus of all privacy regulations is on an individual's right to control access to the personal information that is collected, used (processed) and shared. However, while sharing a common goal of protecting an individual's personal information, the GDPR and US-based Gramm-Leach-Bliley Act[7] (GLBA) differ in approach.

- GLBA, enacted in the US in 1999, indicates that privacy requirements are dependent upon the extent of a financial institution's **continuing relationship with the "consumer"** (i.e., a one-time transaction between financial institution and the consumer would not apply as a continuing relationship). Consumers must also be notified if their information will be distributed to a third party, and in certain circumstances, be presented with an opportunity to opt out of information sharing.
- The GDPR expands what constitutes personal data and mandates that **all institutions maintain the EU resident's right to privacy irrespective of the current relationship** (i.e., heightened security standards apply even after the EU resident cancels their accounts).

These fundamental differences in approach, along with the specific technical requirements outlined in the GDPR, mean that organizations cannot rely on GLBA compliance as an indicator of GDPR compliance. Indeed, firms have to appreciate that GLBA relates mainly to the *sharing* of information, whereas the GDPR relates to the *processing* (collection, use, storage, sharing, retention, etc.) of information. As such, a separate and thorough GDPR assessment is necessary.



[7] Gramm-Leach-Bliley Act, An Act to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, and other financial service providers, and for other purposes, enacted by 106th United States Congress, effective 12 November 1999.

What are some common misconceptions around the GDPR?

There has been a relatively slow response by many non-EU financial services firms to addressing the GDPR. It is difficult to determine what accounts for this general lack of action. It could be that some firms have, incorrectly, viewed the GDPR to be a continuation of existing EU data protection requirements, so no real change is required. Some firms may have seen a May 2018 implementation date and determined there is ample time to act. Some firms – perhaps many – may feel the rule doesn't apply to them, given it's an EU regulation. Some may have assumed their European teams have this in hand – after all, it's an EU regulation

Whatever the reason, more non-EU firms are now starting to realize that the GDPR may apply to them, and when it does, that it is very demanding. As they do, they should be careful about making some common mistakes:

- **Underestimating the level of effort:** often as a result of misunderstanding the breadth, potency and applicability of the GDPR, firms have underestimated the level of effort required to evaluate the applicability of the GDPR, and where it applies, to implement the necessary changes to become compliant. The reality is that the GDPR affects a broad swath of the firm and requires action by a large set of professionals in the businesses and many functional areas (see below). For non-EU firms, it requires a significant degree of cooperation and collaboration between the home office and operations in Europe, as well as with relevant third parties.
- **Underestimating the breadth of impact:** the GDPR may require significant changes to the way firms operate, including their data management strategy, management of customer consents, management and oversight of third parties, the approach to product development, marketing, applications, notifications and other disclosures, potentially firms' business models, the transportation of data across borders, outsourcing contracts and much more. These impacts are likely material and will take time to fully identify, consider and address.
- **Thinking it's easy to identify EU residents:** in practice, it is hard for firms to identify who within their customer base is an EU resident. To the extent that firms have gathered full residentship data, it is easier. Identifying European mailing addresses as primary residences will also help (including non-EU residents living in the EU, as it applies to them, too). Identifying the number of EU residents within the customer base will be a major determinant of the extent to which the GDPR applies and how much of its impact can be quarantined to specific business, geographies and data sets.
- **Viewing the GDPR as only relevant to retail businesses:** given that the requirements center on EU residents' data, some firms may think incorrectly that it only relates to retail businesses. However, some corporate clients – for example, small and medium-sized businesses – often use personally identifiable information, such as personal addresses and tax or national security numbers, as part of their customer data or during the client acceptance process. To the extent they do, that could mean the GDPR applies to businesses serving those clients, as well, depending on whether the firm trips GDPR compliance, as noted above.
- **Viewing it as a one-and-done exercise:** perhaps the most significant challenge is redesigning a firm's privacy and business processes to be able to demonstrate GDPR compliance on an ongoing basis, especially as the business, client base and product portfolio evolve, and to periodically reassess whether GDRP applies to the firm. Getting to a position of GDPR-compliance is the end of the beginning. Compliance is an ongoing responsibility and, if anything, it will be the inability to execute on GDPR commitments (e.g., enabling customer data portability or maintaining customer consents to use the data as required) on an ongoing basis that will put a firm at the most risk of regulatory penalties and/or customer class action suits. Building in sustainable approaches that provide the firm with the necessary flexibility to redesign how it develops and delivers products and services to its customers is most critical.

Which parts of your organization will be most affected?

The GDPR will have a significant impact across a firm's three lines of defense:

First line (business lines and technology)

- **Business lines:** like other risks, the front-line businesses have to own the risks they create, including privacy and data protection. They have to identify, measure, monitor and mitigate the risks associated with the GDPR, implement the privacy principles, and design and maintain necessary and effective controls. They also have to implement enterprise-wide risk management frameworks developed by the second line, including in this context privacy risk, information technology risk, operational risk and overall enterprise risk management.
- **Operations:** those running day-to-day operations have to develop and implement the necessary standards and procedures that secure personal data through the data life cycle and conduct DPIAs to properly understand and manage the inherent risks. They also tend to be the vendor relationship owners, so they have to manage relevant third parties so that they remain in line with the firm's privacy and GDPR requirements and obligations.
- **Technology, security and data:** the technology group will have to consider what changes are required to the technology and data architecture to enable the proper handling, processing and security of relevant customer and employee data. This will include how the data is gathered (and through what channel), processed, stored, transferred (including cross-border and to other firms) and, when necessary, destroyed. Tracking what data is affected will be a significant effort, especially as it relates to customer and account book-of-record, employee or contractor data (e.g., time and reporting systems)[5], personal data used in customer relationship and marketing databases, and so on. The data management strategy that firms may need to adopt to effectively execute against GDPR requirements – in terms of tagging (including geotagging), tracking, anonymizing, encrypting, quarantining and making destroyable (in actuality or in effect) – could be onerous, depending on how the firm determines it will address GDPR compliance. Those driving data analytics activities have consider how they may be affected.
- **Customer relationship management (CRM):** firms will need to re-evaluate their CRM strategy and data management to determine if more client segmentation is required, from a perspective of quarantining EU residents' data and in terms of how customer data is used to target products and services.
- **Innovation and marketing:** product development activities may need to be evaluated to determine how GDPR considerations are built into the new products and services, as well as how customer-facing design activities – such as customer surveys and focus groups – may need to be adapted. Marketing materials will need to be revised to include the necessary disclosures, consents and notifications. Consent is one of the largest areas of challenge, especially around the need to consider whether you can 'grandfather' existing consent or whether you need to run a 'retrospective re-consent' exercise.
- **Procurement and contract management:** procurement and legal teams may need to evaluate existing standard contractual template terms to understand whether amendments are required to meet the GDPR requirements - for example around the 72-hour breach notification and increased obligations on data processors. Organizations will need to identify which vendors are processing personal data and a perform a risk-based prioritization exercise to review existing contracts, identify required legal term changes, and potentially re-negotiate and 're-paper' existing contractual arrangements.
- **Human resources (HR), training and communication:** HR will need to consider if changes are required in regard to how employee or contractor data is segmented and managed, how HR data is reported upon and appropriate

employee rights and consents are managed and adhered to. Working with the relevant functions and businesses, HR will need to re-evaluate the portfolio of awareness-raising, training and education activities and how those activities remain current and effective.

First/second line of defense

- **Third party risk management (TPRM):** given the way in which the GDPR applies to third parties, the second-line TPRM group will need to re-evaluate their third party risk management framework and how the first line is adapting their standards and procedures to align with the GDPR.
- **Surveillance and monitoring:** as noted above, to the extent firms have centralized some of their surveillance activities and in so doing are monitoring activity and behaviors of EU residents, those functions may create GDPR obligations that apply to some or all of the data, depending on how it is processed and stored. The same is true of website traffic and user monitoring activities. Assessing if and how EU resident data is used in these activities will be important to determine applicability, but may also drive firms to segment those activities more than at present to isolate the degree to which those functions are impacted by the GDPR.

  Consideration should be given to the monitoring activities conducted by the second (and sometimes first) line, including anti-money laundering, sanction and fraud surveillance – or broader testing activities – so that those activities are GDPR-compliant, where relevant.

Second line of defense

- **Compliance, privacy and security:** the DPO has a critical role in this regard, working with other functional teams. The compliance function will have to validate that the privacy and data security strategy aligns with legal requirements, annual regulatory reporting requirements and broader compliance reporting and surveillance strategies. Compliance will need to develop a robust monitoring and testing program for GDPR, which can be leveraged by the DPO, among others.

  The privacy groups will need to review and revise data policies, as well as confirm that front-line standards and procedures are in line with those revisions and assess they are implemented effectively (either through reviewing first-line testing or conducting its own). Privacy notices will need updating, along with exemptions, exclusions and disclaimers and personal data definitions. Data breach processes will need evaluating so that the firm can meet its GDPR 72-hour notification requirements, including where breaches occur within third parties. The privacy group will need to confirm that data subject rights and data security standards are adhered to, in light of more demanding GDPR requirements. Privacy and data governance structures and roles and responsibilities will need re-evaluating, including the assignment of data protection officers and their working relationship with chief privacy officers.
- **Risk management:** ultimately, second-line risk, working with the compliance and privacy functions, needs to measure and monitor overall privacy and information-security – working with the DPO, who is directly responsible for monitoring – and set tolerances for such risks within a firm's risk appetite framework. This is particularly important for the GDPR given the potential for material fines and class action legal settlements. Firms will need to re-evaluate privacy-risk reporting in this context.

Third line: internal audit

Internal audit will need to adopt its approach to consider the GDPR within a number of audits, notably:

- Compliance monitoring programs
- Reviews of access processes and procedures
- Overall privacy framework validation

In re-evaluating its coverage model, internal auditors should monitor a distinct set of privacy and compliance key performance indicators, as well as potentially some that are specific to the GDPR. Some firms' internal audit groups may perform pre-implementation advisory audits, given the breadth of the requirements and the potential size of fines and settlements, or build assessments on the implementation of privacy by design principles into other relevant audits they perform.

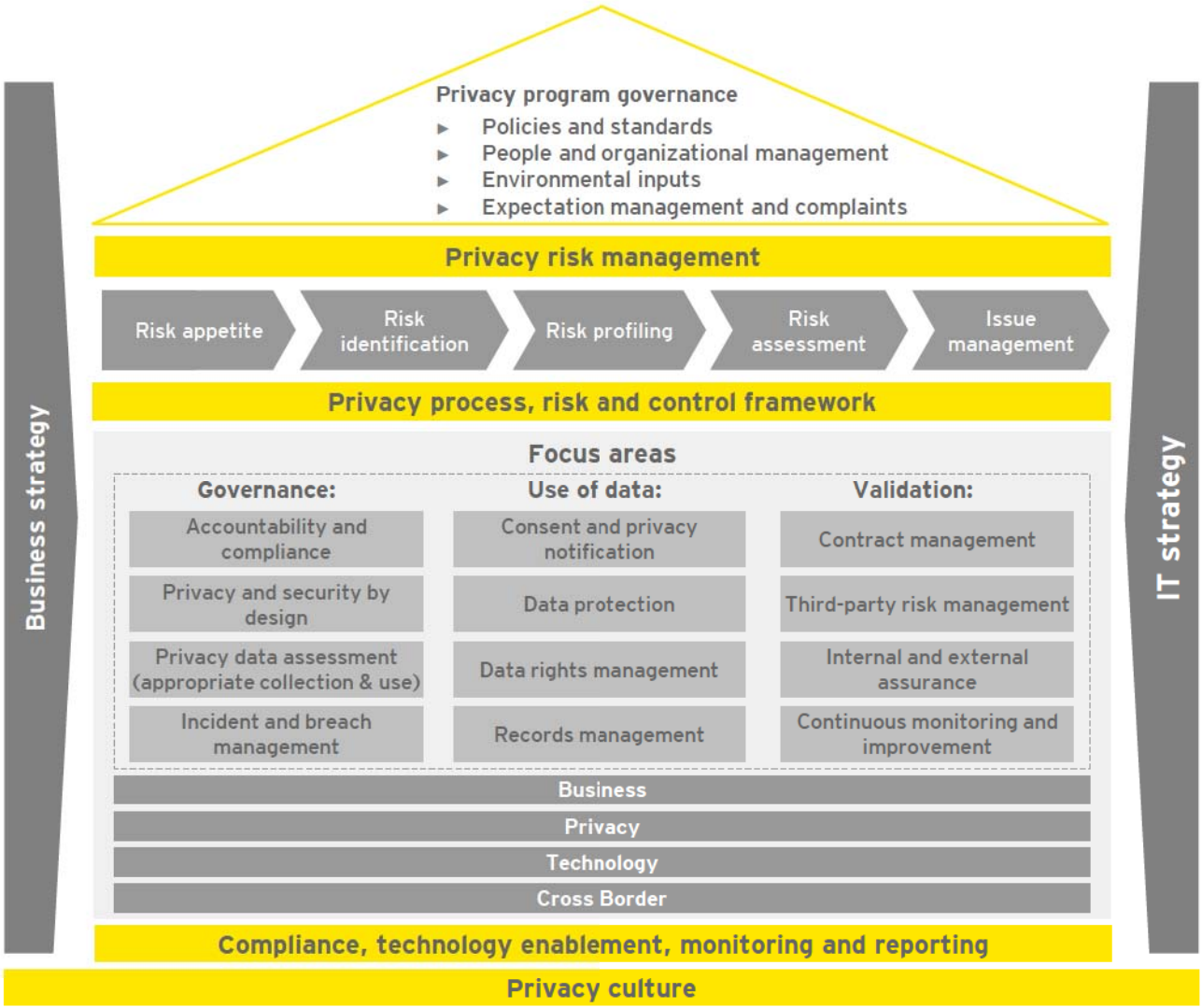
How should you implement the GDPR?

Implementing the GDPR should be viewed as an integrated exercise set within each firm's overall privacy risk management framework. GDPR touches on all aspects of an organization, reaching across people, processes and technology and, as such, establishes a cross-functional team that supports the transformation of the company, which is a critical step for a successful implementation.

EY has developed our own proprietary framework (see figure 2),which links risk management, compliance, privacy and governance with key privacy domains and allows our teams to put privacy in the context of each firm's business and information technology strategy. The framework allows firms to set the privacy strategy within the context of the firm's overall business and IT strategy, and focus on:

- **Program effectiveness:** there has to be an enterprise view of the firm's privacy program, which allows for firm-wide oversight of the program, program-level reporting and escalation, and the application of consistent policy and standards.
- **Privacy risk management:** privacy risk needs to be well managed, in a way that is consistent with the firm's overall risk management strategy, covering the risk life cycle, from risk appetite to risk identification to risk assessment to issues management. The overall privacy framework should link to the firm-wide process and risk and control framework, as well as the third-party risk management program. The various roles and responsibilities across the different lines of defense and functions (compliance, legal, privacy, cyber, etc.) should be clearly defined.
- **Compliance and monitoring:** compliance with relevant rules and regulations should be hardwired into the framework, with robust, ongoing program, compliance and privacy risk reporting to senior management and the board.
- **Data and breach management:** the firm's privacy risk strategy has to be firmly linked to the strategy for managing data, including collecting, processing, storing and destroying data. The data architecture, classification and flows have to enable the firm to conform with its privacy strategy, meet compliance requirements and support customer rights, and meet ever-more challenging incident breach and notification requirements.
- **People and culture:** the talent requirements to properly implement the privacy framework need to be spelled out, and plans need to be in place to confirm the needs are met. This includes the front-line-business talent requirements. After all, those on the front line manage privacy risk on a day-to-day basis. Privacy also needs to be firmly embedded in the firm's culture, with active, ongoing awareness programs and training.

Figure 2: EY's privacy risk management framework



To support business stakeholder understanding of privacy, and the impact of the GDPR on business lines and functions, EY applied its privacy framework to the GDPR and categorized 12 focus areas into 3 themes, as shown in Table 1.

Table 1: GDPR requirements across the EY privacy risk management framework

	Focus area	Desired outcome
Governance	**Accountability and compliance:** privacy operating model, training/awareness, policy development	Creating structures and processes that enable proactive, systematic and ongoing compliance reporting for senior management
	Privacy and security by design: privacy impact assessment, program design based on business model	Achieving risk reduction and management through the application of requirements and tools integrated at various junctures in your process landscape
	Incident and breach management: data incident response plan, 72-hour operational effectiveness process	Enabling rapid management of a data breach, including internal investigations and external reporting
	Privacy data assessment: data use case management/framework, data classification, data flow mapping, data discovery, cloud discovery, high-value asset identification	Establishing and operationalizing governance over personal data usage and analytics as well as understanding the most meaningful attributes of your data that impact compliance risk and optimized use
Use of data	**Consent and privacy notification:** freely given and explicit consent, right to withdraw consent, privacy notices	Increasing transparency through explicit consent to process data and privacy notifications
	Data protection: identify and access management, technology selection, encryption strategy	Approach designed to achieve data protection and enhance your security hygiene
	Data rights management: data subject's right to access, correction, erasure, portability and/or objection	Empowering your organization to support data rights to access, deletion, portability and rectification
	Records management: attach requirements to physical files, electronic documents and emails	Strategy and program design that balances global privacy regulation with data protection, legal and business needs
Validation	**Contract management:** assessment of service-level agreements, assess internal or third-party contracts to identify gaps or identify opportunities to strengthen language	Discovery and revision of contractual provisions pertaining to privacy and security, including data permissions and restrictions
	Third-party risk management: third-party risk assessment, compliance monitoring and data controls	Understanding, designing and monitoring for the management of your third-party personal data access, protection, responsibilities and liabilities
	Internal and external assurance: internal audit assessment, third-party attestation, certification against industry standard	Providing independent confirmation that governance, risk management and internal controls as they relate to both privacy and security are designed and operating effectively
	Continuous monitoring and improvement: compliance monitoring program design, monitoring of key controls, dashboard reporting for management	Designing for ongoing awareness of privacy and security compliance to facilitate risk management and optimization of the control environment

The clock is ticking: act quickly

In enacting the GDPR, the EU gave companies two years to get ready to comply. When enacted, this was viewed as providing sufficient time.

Now, with limited time remaining, many non-EU financial services firms still have a long way to go to validate if the regulation applies to them and, if so, to make all of the necessary changes to be ready for the May 25, 2018, implementation date. Building an approach that is sustainable beyond that date is even more challenging.

Time is of the essence. Non-EU financial services firms need to act quickly.

The first step is assessing applicability; here, a risk-based (not just legalistic) assessment is strongly suggested.

For firms impacted by the GDPR, it is important that the right governance and program structure is put in place from the outset. A cross-functional, cross-business team is required. To be successful and sustainable, this effort cannot be buried in legal and compliance.

A thorough GDPR gap assessment is needed, one that reaches across the swath of affected businesses and functions. To the extent that the assessment is too narrow, it will make timely implementation much harder. Important factors will be identified too late, causing decisions made to degrade the quality of the approach, leave the firm open to regulatory scrutiny and ultimately cost more as work needs to be redone to make the approach sustainable on an ongoing basis.

And, finally, there is a need to prioritize. After all, the timeline to implementation is getting shorter, so firms need to prioritize those activities that get to baseline compliance. Building more sustainable processes can be completed after May 25, as necessary.

It is time to act.

EY contacts

Americas

Cindy Doe
+1 617 375 4558
cynthia.doe@ey.com

John Doherty
+1 212 773 2734
john.doherty@ey.com

Ed Keck
+1 216 583 1296
ed.keck@ey.com

Angela Saverice-Rohan
+1 213 977 3153
angela.savericerohan@ey.com

Mark Watson
+1 617 305 2217
mark.watson@ey.com

EMEIA

Tony de Bos
+31 88 40 72079
tony.de.bos@nl.ey.com

Steve Holt
+44 20 7951 7874
sholt2@uk.ey.com

Asia-Pacific

Jeremy Pizzala
+852 9666 3428
jeremy.pizzala@hk.ey.com

For more cyber and privacy insights, visit ey.com/fsGDPR **or** ey.com/fscyber

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 our organization, please visit ey.com.

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.

EYG no. 05767-171Gbl
1709-2407447 BDFSO
ED None

ey.com