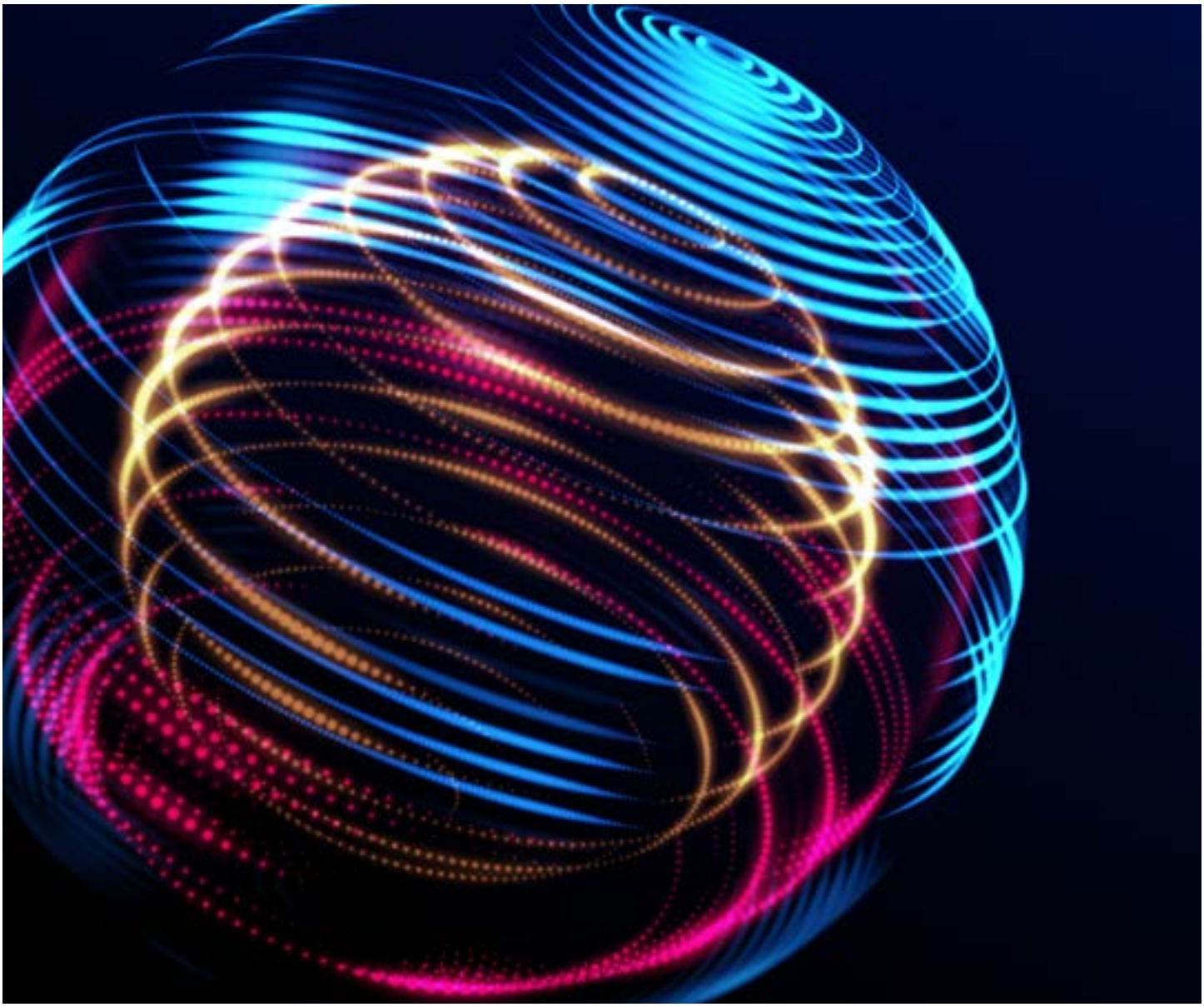
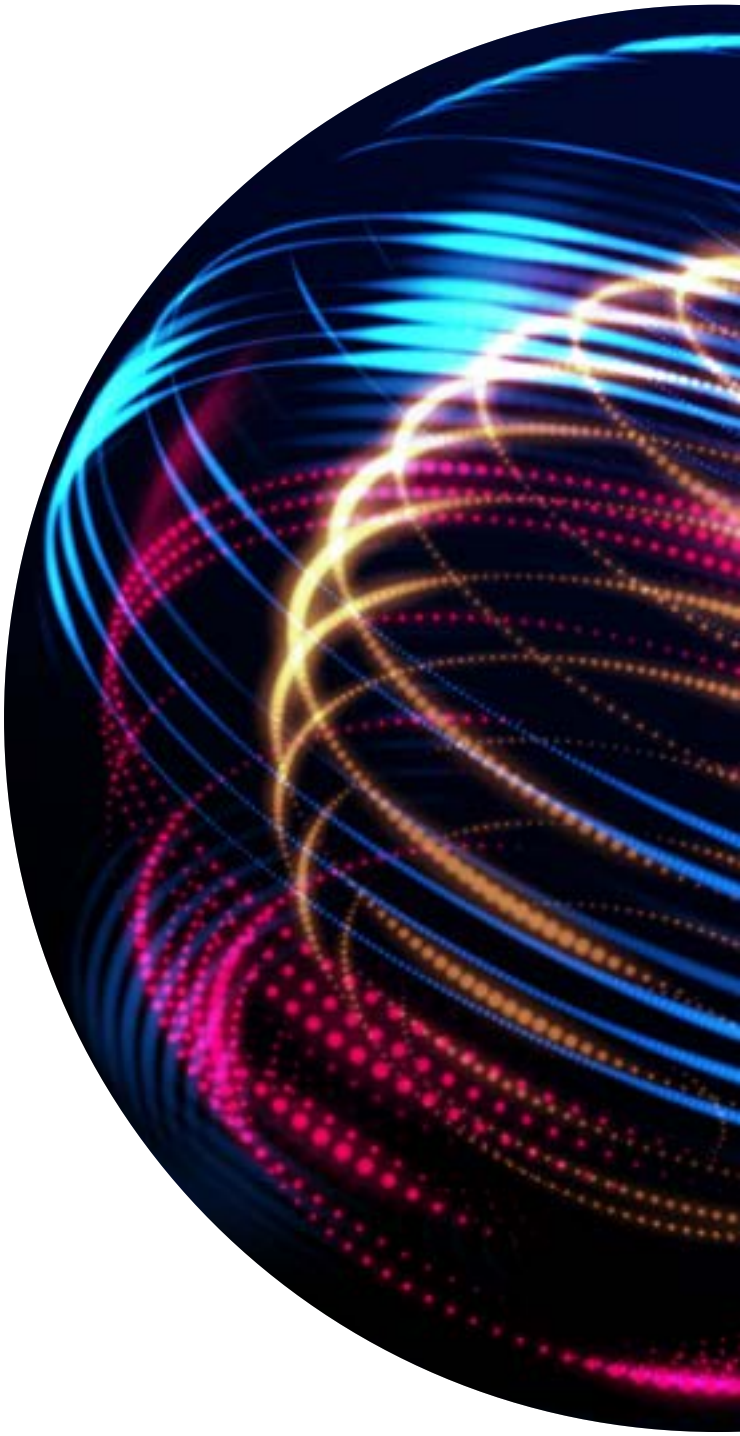
Deloitte.



The shifting landscape of risk: Perspectives on payments companies, Internal Audit, and the pandemic

COVID-19 has changed the way our payments clients operate as well as the risks they face on a daily basis. Our team of Internal Audit (IA) professionals has aggregated lessons learned during this time to illustrate how risks have evolved, and how Payment Services IA shops can enhance their understanding of these changing risks and drive value for their organizations.

Table of contents



COVID-19 and its impact on payments

As COVID-19 continues to affect the globe, consumers are transitioning away from using cash, favoring online or contactless payment methods. In contrast to cash, digital wallets and contactless methods are perceived as safer during a pandemic, accelerating a pre-existing trend toward the adoption of digital payment methods. The accelerated shift to digital payments within the context of COVID-19 further complicates risks posed to financial technology (FinTech) firms, payments processing companies, and their consumers. An understanding of the dynamic environment, both internal and external, is critical for driving value and enabling IA shops to provide assurance, advise the business on risk management practices, and anticipate evolving risks.

We have summarized a number of select risk considerations that our clients have raised as potential concerns affecting payments companies operating in the "next normal" arising from the pandemic. This list is not exhaustive; however, it highlights some of the specific concerns that have arisen at many payments company IA shops since the pandemic began.

- *Fraud Risk*
- *Cyber Risk*
- *Business Continuity*
- *Bank Secrecy Act/Anti-Money Laundering*
- *Safeguarding funds*

Fraud

Fraud and employee misconduct thrive during a crisis, and the increased prevalence of working from home creates a novel environment for fraudulent behavior. Payments companies may be letting their guard down as they focus on reacting to the pandemic by delaying internal audits, reducing headcounts, or implementing long-term work-from-home activities. The shift away from "business as usual" creates vulnerabilities for payments companies during these disruptive times when stress about the future and challenges in the present can run high.

Fraud occurs where **opportunity, motive, and rationalization converge.** The COVID-19 environment creates a perfect storm for these three elements due to the isolation and potential stressors it creates. Payments companies must remain vigilant and actively seek out red flags that may surface in the COVID-19 environment. Temporary or relaxed workarounds, including sharing of remote logins, may allow for theft of confidential data. New and complex government support programs that offer rebates or conditional payouts may encourage fraud or manipulation for financial gain. A work-from-home environment may leave inadequate controls protecting organizational assets more vulnerable to internal or external exploitation. Finally, the time pressure of purchases for a changing operational environment opens up the possibility of fraudulent purchases.

For consumers, there is also an increased risk of fraud due to the shift from in-store to online payments. Though consumers can more easily and conveniently see if an item is available for purchase online, the item may be advertised or sold through a scam effort. There is less transparency when it comes to the integrity of a product because consumers cannot physically see online products. Fraudsters can also obtain online consumer information more easily, as online purchases can be made without needing to show evidence of a physical card (as is the case with a card chip transaction) or authorizing the transaction via the cardholder's signature.

IA considerations may include:

- **How does the COVID-19 environment affect the fraud risk assessment approach and fraud risk landscape?**
- **Are backup personnel (who may need to be activated in response to pandemic-related disruption) prepared for specific fraud-related responsibilities including performing fraud controls activities?**
- **Are segregation of duties set up to prevent fraud in a changing operational environment?**
- **Are additional fraud prevention procedures required during the COVID-19 disruption period?**
- **What is the extent of business disruption for third parties involved in operations and reporting over fraud control activities?**
- **Has the firm considered enhanced fraud monitoring and/or modifications for transaction controls?**

For more information on fraud considerations, please reference Deloitte's COVID-19: Fraud risk considerations in changing control environments paper.

Cybersecurity

Payments companies shifted to the work-from-home model at the onset of the pandemic and are preparing for the post-COVID world where remote employee enablement and productivity continue to be regular and integral to their plans. As payments companies consider how to institutionalize some of the processes and functions quickly put into place in the early months of 2020, cyber security must be a prominent player in all efforts.

Almost overnight, payments companies worldwide found themselves in situations where workers had to shelter and work from home. This created cybersecurity stressors across multiple dimensions, including:

- Increased "Bring Your Own Device" usage
- Secure remote access
- Insecure "ad-hoc" processes
- Compressed timelines for setting up user accounts and onboarding
- Insider threats

Cybersecurity risks have further evolved since the pandemic and the increased use of the work-from-home model. For example, phishing campaigns related to COVID-19 are increasing and are often well disguised as reputable entities. In these cases, cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities and causes. Payments companies should also remain vigilant for scams related to COVID-19. Attacks like these can propagate quickly, extensively impact an entire enterprise network, and result in identity theft with submissions of fraudulent claims for payments and benefit programs.

The opportunity comes in taking lessons learned from what enhanced cybersecurity measures were needed (as well as created) out of necessity and transforming those into the next generation of security and capabilities.

Proactive measures may enhance user experiences and security for remote access, safely enabling opportunities for continued remote work. The proactive approach, in turn, can help mitigate the risk of unprotected devices which could lead to the loss of data, privacy breaches, and systems being held at ransom. Common actions taken by payments companies to address these risks include:

- Enforcing a consistent layer of multi-factor authentication (MFA) or deploying a step-up authentication depending on the severity of access requests
- Ensuring identity and access management processes fully secure third-party identities access networks
- Having a comprehensive view of privileged identities within their IT environments, including a procedure to detect, prevent, or remove orphaned accounts

For more information on cyber considerations, please reference Deloitte's COVID-19: Cyber and the Remote Workforce and Recovering from COVID-19 disruption: Accelerating security imperatives of the future papers.

IA considerations may include:

- **Are remote access controls built to scale?**
- **How are organizations raising awareness, bolstering threat detection, and promoting proactive identification of malicious activity?**
- **How are organizations tracking third-party security plans to prioritize access availability of services?**
- **Are hand-held devices being used more as people work remotely and, if so, are they secure and controlled?**
- **Does the organization have sufficient and appropriate licenses in place to cover greater use of tools, technology, and software to support remote working?**
- **How is the organization monitoring malicious or inadvertent insider threat risk caused by disgruntled or displaced employees and contractors?**
- **How is the organization monitoring the increased use of collaboration tools and other, often unapproved and unmanaged, software-as-a-service (SaaS) applications (Shadow IT)?**
- **How is Management planning for the security imperatives of the future including considerations for gig workers and a largely remote workforce?**

Business continuity and disaster recovery

The disruption from the COVID-19 pandemic provided a real-world test of business continuity plans (BCPs) across the payments industry. The data gathered from this experience provides valuable information that can be used to strengthen BCPs and planning for future disruption.

In some jurisdictions, reopening efforts are being scaled back due to the continued proliferation of the virus. Other jurisdictions face the risk of a resurgence of the COVID-19 virus as reopening efforts continue. On the global level, governments have had varying degrees of success in limiting the spread of the virus. Payments companies must consider BCPs in the context of prolonged measures to combat the virus in some jurisdictions, and a potential second wave of COVID-19 infections in others. It is reasonable to assume that, in these circumstances, public health officials and companies alike may take measures to promote the safety of their workers, such as imposing renewed stay-at-home orders and limiting travel. While payments companies now have practical experience responding to these measures, the risk of additional disasters or disruptions while a quarantine is in effect presents new operational challenges that many firms traditionally faced.

Additional disasters and disruptions have occurred during prolonged pandemic conditions, and may continue to occur going forward. Hurricane season in North America begins in June and runs through November (2020 brought 29 named tropical storms or hurricanes as of October [1]). Typhoon season in Asia begins in May and ends in October. Volcanic eruptions and earthquakes (such as the 5.3-magnitude quake that hit Croatia earlier this year) are unpredictable and may happen at any time. How can payments companies prepare for any of these events while the majority of its workforce is under quarantine?

Going forward, payments companies should update BCPs to consider how they would respond to disruptions while methods to counter COVID-19's effects are in place. Scenario analysis can be performed to play out how responses would be implemented during a period of multiple, concurrent disruptions. Planning should consider both in-house competencies/technology and activities outsourced to vendors. Many payments companies outsource functions such as customer support and business processing to vendors that are geographically dispersed. Lessons learned from COVID-19 should be rolled forward to plan for concurrent disruptions affecting both in-house and outsourced operations.

Finally, enhanced BCPs and scenario analysis present an opportunity for the operations and finance arms of payments companies to collaborate on risk management and mitigation. Planning for disruptive scenarios may include assumptions around the failure of one or more key controls. Assuming multiple control failures, payments companies can model the impact that disasters and disruptions may have on their business, both from a financial and operational perspective. This view allows payments companies to better prepare a detailed and informed BCP that protects the financial heath and viability of the business.

IA considerations may include:

- What lessons learned or control failures were identified during the execution of BCP for COVID-19?
- What action plans were initiated to make improvements to the process, and what is the implementation status of these plans?
- Where are key operations (in which disruption may have a regulatory or customer facing impact) located, and/or are key operations now dispersed due to the work from home environment?
- What are the main disaster risks in areas where key operations and related personnel are located?
- Have key third parties been taken into consideration as part of the BCP?
- How have BCP plans and controls been updated to consider execution now that employees are working remotely?

1. https://www.nhc.noaa.gov/archive/tws/

Bank Secrecy Act/Anti-Money Laundering (BSA/AML)

With the rush to get relief to small businesses through the CARES Act in the US, the Paycheck Protection Program (PPP), which provided loans to small business for the purpose of keeping employees on the payroll, came with unforeseen challenges. PPP was designed to originate and disburse loans quickly, and as the nation continues to deal with the impacts of COVID-19, payments companies who participate in making disbursements under the program (and any similar programs in the future) must be able to allocate sufficient resources to meet BSA/AML obligations.

The rapid disbursals associated with government stimulus programs require payments companies to have a strong understanding of beneficial ownership requirements for new and existing customers. For existing customers, payments companies can leverage existing Know Your Customer (KYC) programs to manage beneficial ownership information and risk requirements. For new customers, institutions should still follow existing processes for onboarding but may face added time pressures, especially around the validation of beneficial ownership. Payments companies may need to tweak onboarding processes to be able to meet the requirements for quickly establishing an understanding of new customers beneficial ownership relationships, including confirmation of authorized signers.

Risk rating is a mandated part of the customer onboarding process. The Customer Due Diligence (CDD) Rule requires payments companies to conduct due diligence in order to understand the nature and purpose of the customer relationship. For loans distributed by payments companies which are associated with PPP or other stimulus packages, payments companies should consider if the new loan or any changes to information in the existing KYC file have an impact on the overall risk rating assigned to the customer. Changes to BSA/AML programs may include additional due diligence requirements or enhanced due diligence, which can stress operations during a disruptive, work-from-home environment and may present new risks of non-compliance.

For more information on PPP and BSA/AML considerations, please reference Deloitte's CARES Act Paycheck Protection Program: anti-money laundering considerations paper.

IA considerations may include:

- How do government stimulus programs affect the requirements for BSA/AML and KYC programs?
- What operational changes are needed to meet the demands of customers requesting new or modified loans?
- How is the payments company set up to perform BSA/AML and KYC activities in a remote work environment?
- Are measures taken to provide sufficient resources to manage backlog and ensure quality?
- Are BSA/AML programs adequately staffed if future stimulus funding becomes available?

Safeguarding of funds

Payment processing requires payments companies to hold customer funds, whether pooling funds for settlement or through offering stored value accounts to their customers. Regulations currently exist to set rules on how to safeguard those funds through insurance or surety bonds as a condition to operating under a payments license. Payments companies have historically operated under these rules in the normal course of business. The effects of COVID-19 on business has been anything but normal.

As already stated, a positive trend for payments companies is the increased adoption of digital and contactless payment methods by society at large. It appears that the pandemic has accelerated a longstanding trend of increased digital payment volumes driven by technological innovation and demographic change.

An increase in the number of users and volume of payments processed through payments companies also means an increase in the amount of funds that need to be safeguarded. While this is a good problem to have, it requires payments companies to be vigilant and closely monitor volumes against safeguarding rules. Arrangements should be made to proactively model volume trends and use that information to ensure continual compliance with license requirements.

Payments companies should also be on the lookout for changing requirements as regulators gain an understanding of how the financial health of institutions was affected during the pandemic. While payments companies may not hold loans or maintain trading desks, larger financial services firms with these capabilities may drive changes to the regulatory environment's safeguarding rules that affect payments companies. This is particularly important for payments companies that have a global footprint, as different jurisdictions may vary in how aggressively changes to current rules are pursued and how stringent those new requirements may be. Vigilance over the regulatory landscape helps drive ongoing compliance in times of change.

IA considerations may include:

- Have there been any changes to safeguarding requirements in the jurisdictions where products and services are offered, including internationally?
- What are the allowable methods for safeguarding funds in applicable jurisdictions?
- How does management monitor funds to identify when changes are needed to insurance/bond coverage amounts?
- Are there controls or early warning indicators in place to prompt actions to avoid non-compliance?
- How quickly can coverage amounts be increased if the need to do so is identified?

Risk assessment

Changes that arise from the impacts of COVID-19 create an opportunity for payments companies to re-assess and improve their risk management processes. Importantly, the disruption created by COVID-19 can shine a light on the effectiveness of controls and other preparations taken using the Three Lines Model to mitigate risk. A revamped risk assessment that takes new and emerging risks into consideration is a critical starting point for IA to understand how risks manifest in the new environment. This is especially important for payments companies venturing into new offerings in response to the pandemic, as risk management plays an integral role in building and maintaining stability.

A leading practice is to perform a continuous risk assessment to keep a pulse on new and emerging risks as they manifest themselves. For payments companies that have not yet stood up a continuous risk assessment process, management should consider performing an off-cycle assessment to attain a dynamic, current view of how risks impacted by COVID-19 and related control activities (or lack thereof) influence the overall risk profile of the company. This is akin to an off-cycle assessment driven by a triggering event (such as a new product launch) and allows management to identify potential issues and develop action plans to mitigate or avoid emerging risks altogether.

One takeaway from the current environment is that business-as-usual can—and did—change overnight, and payments companies that can better predict potential risks will likely have an advantage. Knowing the severity of a risk and having a plan to mitigate it is equally important. Either by necessity or by design, payments companies that respond to COVID-19 by strengthening risk management and risk assessment practices may lock in an investment that should continue to pay off once the pandemic subsides.

IA considerations may include:

- **Were material changes made to business processes, or did volumes shift between existing processes?**
- **Has human capital been able to keep pace with the rate of changes?**
- **What issues were uncovered since the pandemic, and have remediations for these issues been validated?**
- **What are the trends observed in how customers are using services, and how may that influence the future risk profile?**
- **Is the business reliant on a specific subset of vendors, such as those in the travel and hospitality industry, for major revenue streams?**
- **Do changes in consumer behavior during the pandemic threaten sources of revenue?**

Conclusion

As customers continue to transition away from cash, payments companies should be aware of how their risk profiles may be changing within the context of COVID-19. New **fraud risks** and **cyber risks** are emerging that affect the way that payments companies operate. Existing **business continuity** programs and **BSA/AML** programs may no longer be sufficient for the payments company's needs. Throughout all the changes, payments companies are still expected to **safeguard customer funds** and provide the same level of service as in the past. Through **understanding and assessing the changing risk environment**, Internal Audit can enhance its organization's risk management capabilities and allow payments companies to thrive through the duration of the COVID-19 pandemic and into whatever comes next.

How can Deloitte assist?

Deloitte's Risk & Financial Advisory's Payments group provides advisory and internal audit assistance to companies that offer innovative payments solutions to consumers and small businesses. Our team includes industry veterans and former regulators who bring first-hand knowledge and experience with regard to risk management, compliance, and internal audit to payments companies. We bring deep industry knowledge and resources to advise our clients and can assist in design operationalization, staff augmentation, and data analytics testing support related to their dynamic business needs.

Contact us

Andreas Tsalikis
Partner
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
atsalikis@deloitte.com

Maria Marquez
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
marmarquez@deloitte.com

Daniel Korda
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
dkorda@deloitte.com

Konstantine Loukos
Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
kloukos@deloitte.com