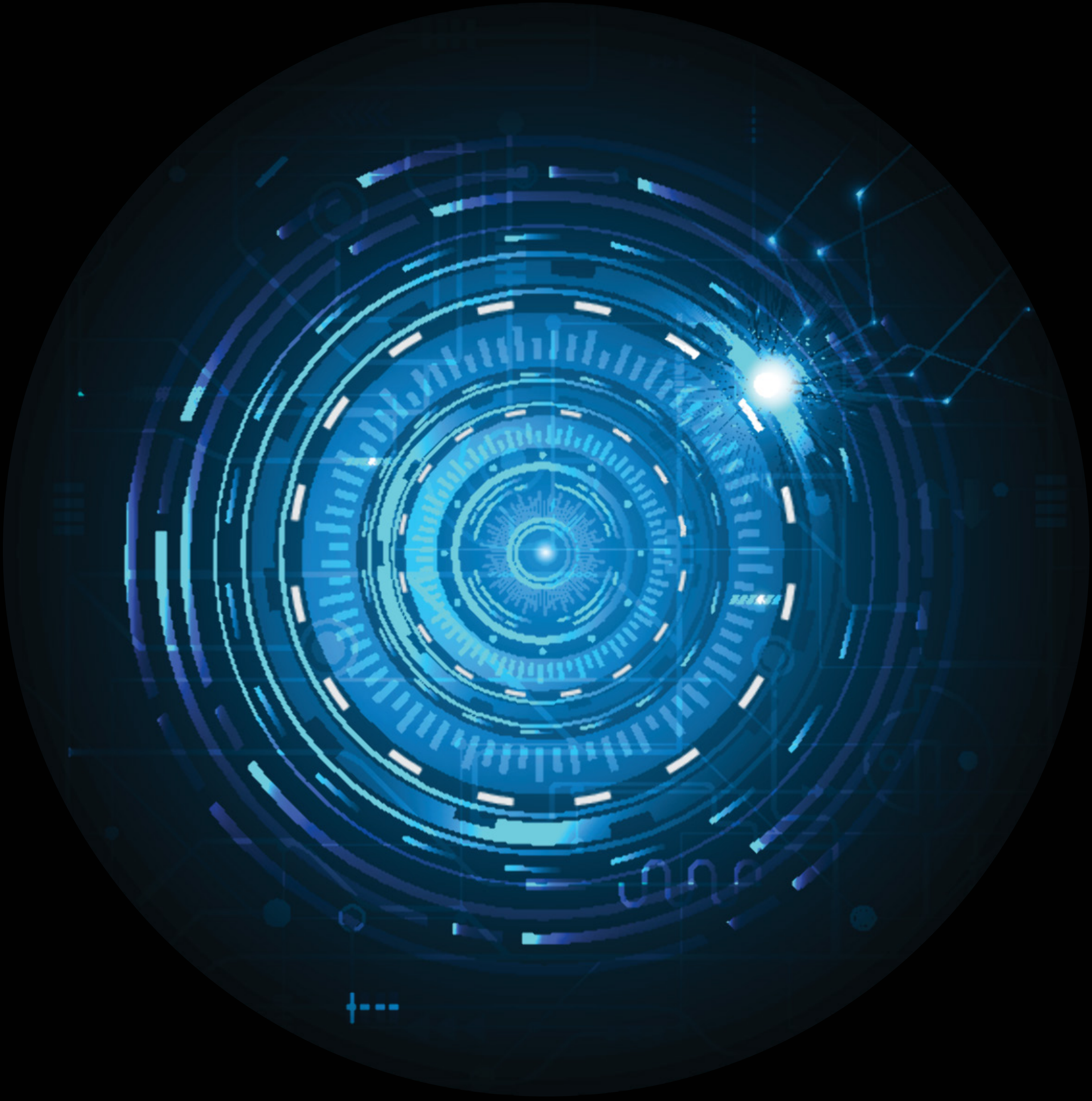
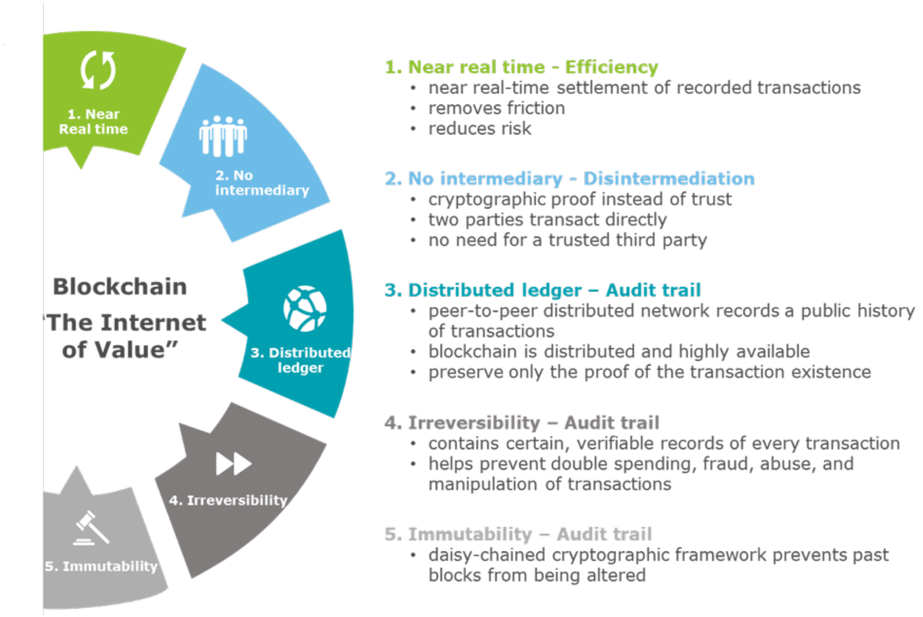


Blockchain risk management

Risk functions need to play
an active role in shaping
blockchain strategy

Is your organization prepared for the new risks posed by the introduction of a blockchain framework?

The successful adoption and operation of any new technology is dependent on the appropriate management of the risks associated with that technology. This is especially true when that technology is more than an application and is part of the organization's core infrastructure, as is the case of Distributed Ledger Technologies (DLT). DLTs have the potential to be the backbone of many core platforms in the near future. DLT is a peer-to-peer (or machine-to-machine) value-transfer framework that provides Byzantine fault tolerance with distributed databases updated with a consensus mechanism. Every participant node has an exact copy of the data and a consensus protocol synchronizes the updates across participant nodes.



1. Near real time - Efficiency
- near real-time settlement of recorded transactions
- removes friction
- reduces risk

2. No intermediary - Disintermediation
- cryptographic proof instead of trust
- two parties transact directly
- no need for a trusted third party

3. Distributed ledger – Audit trail
- peer-to-peer distributed network records a public history of transactions
- blockchain is distributed and highly available
- preserve only the proof of the transaction existence

4. Irreversibility – Audit trail
- contains certain, verifiable records of every transaction
- helps prevent double spending, fraud, abuse, and manipulation of transactions

5. Immutability – Audit trail
- daisy-chained cryptographic framework prevents past blocks from being altered

The blockchain protocol is a special case of DLT, where the consensus protocol creates a daisy chained immutable ledger of all transactions that is shared across all participants. This framework allows for near real-time value transfer (e.g. assets, records, identity) between participants without the need for a central intermediary. Any transfer of value between two parties and the associated debits and credits are captured in the blockchain ledger for all parties to see. The cryptographic consensus protocol ensures immutability and irreversibility of all transactions posted on the ledger.

Risk practitioners across sectors are very excited about blockchain's promise to help organizations minimize—and in some cases eliminate—the risks posed by current systems. Blockchain is being viewed as the foundational technology for the future of risk management. However, as the technology continues to mature and many theoretical use cases begin to get ready for commercialization, it behooves the industry to start focusing on a less discussed question: "Do blockchain-based business models expose the firm and market to new types of risk? If so, what should firms do to mitigate these risks?" It's critical for firms to understand that while blockchain promises to drive efficiency in business processes and mitigate certain existing risks, it poses new risks to the firm and market. Additionally, it's important to understand the evolution of regulatory guidance and its implications. Earlier this year, the Financial Industry Regulatory Authority (FINRA) issued detailed guidance[1] on some of the operational and regulatory considerations for developing various use cases within capital markets. Firms need to ensure that these regulatrory requirements are addressed in the blockchain based business models.

Types of blockchains and inherent risks

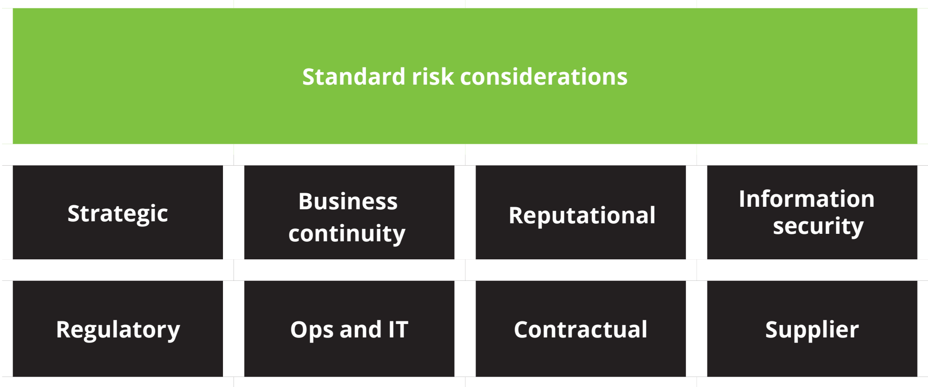
Blockchains fall under two types: permissionless and permissioned chains. Permissionless blockchains allow any party without any vetting to participate in the network, while permissioned blockchains are formed by consortiums or an administrator who evaluate the participation of an entity on the blockchain framework.

Permissionless blockchains start out with a pool of crypto currency to pay service providers, or miners, to participate in the process. Miners are service providers who update the general ledger with transactions that occurred between participants. Anyone can participate as a miner as long as they meet certain technological requirements dictated by the network. No other entity checks, such as know your customer (KYC) or other background checks of the service provider, are possible in this framework. Anyone acquiring this crypto currency on the blockchain framework can transact with any entity on the blockchain. As such, there is increased risk of money laundering and theft of currency from a user's blockchain account on that network. Additionally, permissionless blockchains have scalability and privacy issues that pose a significant risk to the use of this framework by financial institutions.

Permissioned blockchains do not have the crypto currency requirement as the consortium network or the administrator can predefine the update process without the use of unvetted service providers. Usually, this involves a choice of a consensus algorithm that is deployed on the network to update the blockchain ledger. Additionally, scalability and privacy issues can be handled by the choice of infrastructure by the participants, and suspicious activity monitoring can be deployed across the network by the administrator or the consortium. Therefore, this framework is more suitable for institutions to use with a group of known and predetermined peers.

Regardless of the type of blockchain, the business logic is encoded using smart contracts. Smart contracts are self-executing code on the blockchain framework that enable straight-through processing, which means that manual intervention is not required to execute transactions. Smart contracts rely on data from outside entities referred to as "oracles," and can act on data associated with any public address or with another smart contract on the blockchain. A smart contract can mimic a contract and can execute the contract automatically if conditions required to consummate the contract have been met. Smart contracts are generally the most vulnerable points for cyberattack and technology failures. Like any other software code, smart contracts require robust testing and adequate controls to mitigate potential risks to blockchain-based business processes. Firms across different industries are investing heavily in this new technology to build a variety of use cases on topics such as identity management, provenance, trade finance, clearing and settlement, cross-border payment, etc. While the blockchain technology promises to drive efficiency or reduce cost in each of the use cases, the blockchain, as well as the smart contracts encoding the business logic, have certain inherent risks. It's imperative that firms understand the risks and the appropriate safeguards to reap the benefits of this technology. Failure to mitigate the risks posed by adopting the new technology might undermine all the benefits. These risks can be broadly classified under three categories: standard risks, value transfer risks, and smart contract risks.

Standard risk considerations



Standard risk considerations

Strategic

Business continuity

Reputational

Information security

Regulatory

Ops and IT

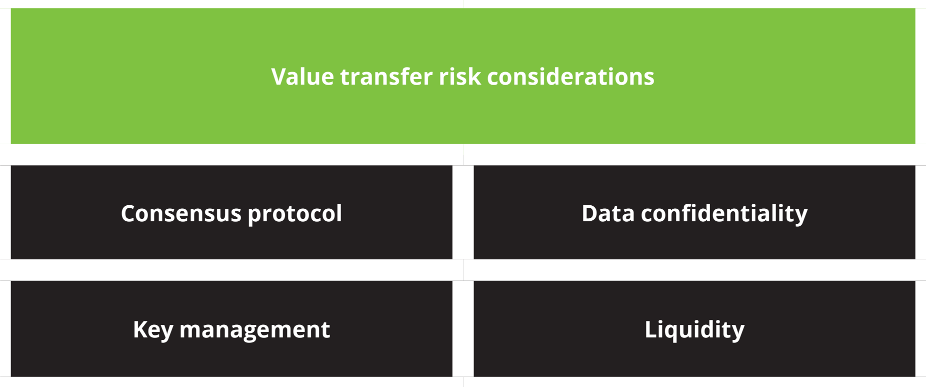
Contractual

Supplier

Blockchain technologies expose institutions to risks that are similar to those associated with current business processes but introduce nuances for which entities need to account:

- **Strategic risk:** First, firms need to evaluate whether they want to be at the leading edge of adoption or wait to adopt until the technology matures. Each of these options have varying levels of risks to business strategy. Second, given the peer-to-peer nature of this technology, it's important for entities to determine the right network to participate in, as their business strategy could be impacted by the different entities participating on the chain. Third, the choice of the underlying platform could pose limitations in the services or products that can be delivered via this platform.
- **Business continuity risk:** Blockchain technologies are generally resilient due to the redundancy resulting from the distributed nature of the technology. However, the business processes built on blockchains may be vulnerable to technology and operational failures as well as cyberattacks. Firms need to have a robust business continuity plan and governance framework to mitigate such risks. Additionally, blockchain solutions shorten the duration of many business processes, and business continuity plans should account for a shorter incident response and recovery time.
- **Reputational risk:** Unlike fintech applications, blockchain technology is part of core infrastructure and will have to work seamlessly with legacy infrastructure. Failure to do so could result in poor client experience and regulatory issues.
- **Information security risk:** While blockchain technology provides transaction security, it does not provide account/wallet security. The distributed database and the cryptographically sealed ledger prevents any corruption of data. However, value stored in any account is still susceptible for account takeover. Additionally, there are cyber security risks to the blockchain network if a malicious actor takes over 51 percent of the network nodes for a duration of time, especially in a closed permissioned framework.
- **Regulatory risk:** Currently, across the globe there's uncertainty around the regulatory requirements related to blockchain applications. Additionally, there may be regulatory risks associated with each use case, the type of participants in the network, and whether the framework allows domestic or cross-border transactions. This could also include cross-border regulations related to privacy and data protection. FINRA's regulatory guidance[2] calls for broker-dealers to be cognizant of all applicable federal and state laws, rules, and regulations when exploring issuing and trading securities, facilitating automated actions, and maintaining transactions on a DLT network. In its guidance, FINRA highlights DLT's potential to affect various aspects of the securities market, including market efficiency, transparency, post-trade processes, and operational risk.
- **Operational and IT risks:** Existing policies and procedures will need to be updated to reflect new business processes. Additional technology concerns could include speed, scalability, and interface with legacy systems in implementing the technology.
- **Contractual risk:** There will likely be several service-level agreements (SLAs) between participating nodes and the administrator of the network, in addition to SLAs with service providers that will need to be monitored for compliance.
- **Supplier risks:** Firms may be exposed to significant third-party risks since most of the technology might be sourced from external vendors.

Value transfer risk considerations



Value transfer risk considerations

Consensus protocol

Data confidentiality

Key management

Liquidity

Blockchain enables peer-to-peer transfer of value without the need for a central intermediary. The value transferred could be assets, identity, or information. This new business model exposes the interacting parties to new risks which were previously managed by central intermediaries.

- **Consensus protocol risk:** The transfer of value in a blockchain framework occurs by the use of a cryptographic protocol that arrives at a consensus among participant nodes to update the blockchain ledger. There are several such cryptographic protocols that are used to achieve consensus among participant nodes for updating the blockchain ledger. Each such protocol will have to be evaluated in the context of the framework, the use case, and network participant requirements.

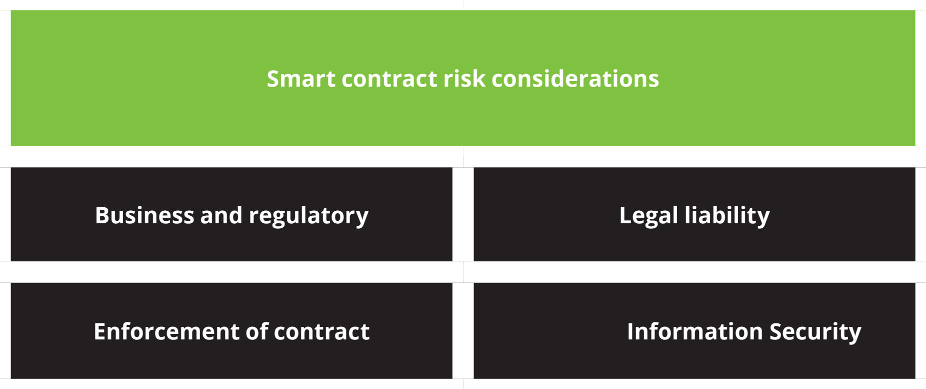
  For example, the practical Byzantine fault tolerance algorithm requires parties to agree on the exact list of participants, and membership in the system is set by a central authority or closed negotiations. In a proof-of-stake consensus protocol, it's possible for block generators to vote for multiple blockchain histories, which may lead to consensus never resolving and thus, ledger would not complete the transfer of value.

- **Key management risk:** While the consensus protocol immutably seals a blockchain ledger and no corruption of past transactions is possible, it's still susceptible to private keys theft and the takeover of assets associated with public addresses. Digital assets could become irretrievable in the case of accidental loss or private key theft, especially given the lack of a single controller or a potential escalation point within the framework.

- **Data confidentiality risk:** The consensus protocol requires that all participants in the framework can view transactions appended to the ledger. While the transactions in a permissioned network could be stored in a hashed format so as to not reveal the contents, certain metadata will always be available to network participants. Monitoring the metadata can reveal information on the type of activity and the volume associated with the activity of any public address on the blockchain framework to any participant node.

- **Liquidity risk:** The Bank for International Settlements warned that the adoption of DLT, such as the blockchain, may introduce new liquidity risks.[3] In current business models, intermediaries typically take on the counterparty risks and help resolve disputes. Dispute resolution in a distributed trust environment is a requirement that will rely on preordained arrangements.

Smart contract risk considerations



Smart contract risk considerations

Business and regulatory

Legal liability

Enforcement of contract

Information Security

Smart contracts can potentially encode complex business, financial, and legal arrangements on the blockchain, and could result in the risk associated with the one-to-one mapping of these arrangements from the physical to the digital framework. Additionally, cyber security risks increase as the smart contracts rely on outside oracles to trigger contract execution.

- **Business and regulatory risks:** Smart Contracts should accurately represent business, economic, and legal arrangements defined between parties in the framework. The smart contracts that are defined on a blockchain network will apply in a consistent manner to all participants across the network. Therefore, these smart contracts will have to be capable of exception handling, and the consequences of these exceptions in the form of a programmatic output on the blockchain framework will have to be tested across the universe of all other smart contracts within the network for adherence to business and legal arrangements and compliance with regulations.
- **Contract enforcement:** Currently there is no legal precedent around the enforcement of a smart contract in lieu of a physical contract. And there are no regulations governing smart contracts. Also, as the data on a blockchain framework is immutable, care should be taken to amend smart contracts to avoid breaches of existing regulation by acting on data from the past on the blockchain that are not within the statutory legal limits for a financial arrangement.
- **Legal liability:** In a permissioned network, the legal liability remains unclear for an improper, erroneous, or a malicious administration of a smart contract resulting in a transaction with two or more entities on the network, causing assets to leave the network via those transacting entities.
- **Information security risks:** Smart contracts may be susceptible to security breaches and improper administration. Participant entities or the network administrator will need a strong governance and change control process to deploy new or amend existing smart contracts. They will also need a robust incident management process to identify and respond to glitches in smart contract operations.

Oracles are entities that exist outside the blockchain framework but feed data to the network, which could trigger the execution of the smart contracts within the network. The biggest risk to a blockchain framework may lie within these oracles as these could be subject to malicious attacks to corrupt the data being fed to the blockchain. This could cause a catastrophic domino effect across the entire network.

Conclusion

The blockchain peer-to-peer framework offers the potential to transform current business processes by disintermediating central entities or processes, improving efficiencies, and creating an immutable audit trail of transactions. This provides the opportunity to lower costs, decrease interaction or settlement times, and improve transparency for all parties. This transformational framework could alter the way financial institutions conduct business as many transactions are peer to peer in nature.

While the benefits are clear, there are myriad risks that may be imposed by this nascent technology. Understanding of the blockchain technology and its associated risks articulated in this paper may change and evolve as this technology continues to mature. It's therefore imperative for all organizations to continue to monitor the development of this technology and its application to various use cases.

Blockchain technology will transform business models from a human-based trust model to an algorithm-based trust model, which might expose firms to risks that they have not encountered before. In order to respond to such risks, firms should consider establishing a robust risk management strategy, governance, and controls framework.

Components of an effective blockchain risk management framework

Risk management framework

Business objectives	Growth / innovation	Client experience	Cost reduction	Improved time to market	Risk and compliance management
Core processes, supporting functions	Information technology	Human resources	Compliance	Finance	Other

	Standard risk considerations				Value transfer risk considerations		Smart contract risk considerations	
Risk considerations	Strategic	Reputational	Business continuity	Security	Consensus protocol	Data confidentiality	Business and regulatory	Legal liability
	Regulatory	Ops and IT	Contractual	Supplier	Key management	Liquidity	Enforcement of contract	Governance

Operating model components	Governance and oversight	Policies and standards	Management processes	Tools and technology	Risk metrics and reporting	Risk culture

1. Distributed Ledger Technology: Implications of Blockchain for the Securities Industry, January 2017: https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf

2. ibid

3. Distributed Ledger Technology in payment, clearing and settlement, February 2017: http://www.bis.org/cpmi/publ/d157.pdf

Contacts

Authors

Prakash Santhana
Managing Director
Deloitte Risk and Financial Advisory
Deloitte and Touche LLP
30 Rockefeller Plaza
New York , NY 10112-0015
+1 212 436 7964
psanthana@deloitte.com

Abhishek Biswas
Senior Manager
Deloitte Risk and Financial Advisory
Deloitte and Touche LLP
30 Rockefeller Plaza
New York , NY 10112-0015
+1 212 436 6398
abiswas@deloitte.com

Contributors

Eric Piscini
Principal
Deloitte Consulting LLP
191 Peachtree Street
Suite 2000 Atlanta , GA 30303-1749
+1 404 631 2484
episcini@deloitte.com

Yang Chu
Senior Manager
Deloitte Risk and Financial Advisory
Deloitte and Touche LLP
555 Mission Street
San Francisco, CA 94105-0920
+1 415 783 4060
yangchu@deloitte.com

Swagatam Chakraborty
Senior Consultant
Deloitte Risk and Financial Advisory
Deloitte and Touche LLP
100 Kimball Drive
Parsippany, NJ 07054
+1 973 602 6000
swchakraborty@deloitte.com

Livia Lima Fava
Senior Consultant
Deloitte Risk and Financial Advisory
Deloitte and Touche LLP
30 Rockefeller Plaza
New York , NY 10112-0015
+1 212 492 4456
llimafava@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Deloitte.