The new and/or emerging risks that management and Boards of Directors face today include those arising from rapid transformation in the delivery of technological solutions, including dramatic changes resulting from the increased use of “cloud” computing. In today’s environment, enterprise risk management (“ERM”) and crisis-management have become imperative for management and Boards of Directors. The consequences of risk arising from the rapid change in technological solutions that need to be addressed by a company in order to reduce exposure to potential adverse consequences may include, without limitation, those relating to business interruption, security/privacy, data integrity, intellectual property, licensing, records retention, electronic discovery, export control and other violations of law in both the US and foreign jurisdictions.

Failure to identify, assess, prioritize and mitigate potential risks can lead to action by federal, state, and foreign regulatory authorities, including the US Securities and Exchange Commission, US Department of Justice, Congressional investigators, and states attorneys general. It can also lead to civil litigation, political attention, unfavorable press, loss of business and unfavorable competitive positions.

In an earlier client alert (Effective Enterprise Risk Management and Crisis Management), we noted generally that it is essential to have robust ERM programs and governance processes in place at the management and Board levels to identify, assess, prioritize and mitigate risks and to have a plan in place to manage risks if they materialize. The earlier Client Alert noted that Boards and management have a responsibility to ensure that these processes are in place. Changes to the delivery of technological solutions, including, cloud computing, create significant emerging risks that must be a part of an ERM plan. Those risks must be identified and assessed as part of the business decision to either retain current technological solutions or move to alternative methods, such as cloud computing. Risk assessment and mitigation should be incorporated into the ERM process and crisis management plan.

This client alert focuses on guidance released by the Committee of Sponsoring Organizations of the Treadway Commission (“COSO”) on June 20, 2012 to facilitate the application of ERM to address risks associated with cloud computing. The paper, entitled “Enterprise Risk Management for Cloud Computing” (“ERM for Cloud Computing” or the "paper") discusses the application of the principles set forth in COSO’s seminal “Enterprise Risk Management - Integrated Framework” (“Integrated Framework”) to the cloud computing assessment process. The paper provides an ERM framework for identifying, monitoring, mitigating and/or accepting risks relating to the rapid development of cloud computing.

ERM for Cloud Computing represents an important example of how a company’s broad approach to ERM under the original Integrated Framework can be used by companies in an ERM approach to cloud computing. The paper, however, also provides important guidance that may be used to address other rapid changes occurring in the marketplace, including, developments that implicate significant legal, regulatory, technological, operational or other transformational changes (e.g., use of social media). Thus, the paper also provides guidance on an ERM process that may be useful across a broad range of industries and processes that are impacted by significant and rapid
changes, such as health care entities that need to address significant regulatory and technological changes required in connection with (i) the implementation, update or assessment of electronic medical records ("EMR") or (ii) the conversion of systems required to move to International Classification of Diseases, Tenth Revision ("ICD-10"), or (iii) the development of required responses to other significant changes imposed under health care reform.

The paper also emphasizes the increasingly large role of the legal and regulatory framework that must be incorporated within ERM and the underlying processes, procedures and systems that comprise the resulting internal control framework. It underscores the need to ensure that the ERM approach incorporates a multi-disciplinary team that includes the legal and compliance function as well as information technology ("IT"), financial, business and other operational functions.

**Background**

COSO is a joint initiative of the Institute of Internal Auditors, the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International and the Institute of Management Accountants. COSO is recognized as a world-wide leading authority on ERM, internal controls and fraud deterrence.

COSO developed the paper in order to facilitate the development of an ERM approach to respond to the significant rise of cloud computing during recent years. The paper reports that over 3 million businesses were customers of Google's cloud service offerings as of 2010. The paper also indicates that cloud computing is projected to comprise a $140 billion industry by 2014. The paper defines "cloud computing" at a very high-level as "a computing resource and deployment model that enables an organization to obtain its computing resources and applications from any location via an Internet connection." The hardware, software and data used in the cloud computing process resides in a technology center shared with other organizations (rather than residing on the company's own infrastructure). The technology center is managed by a third-party vendor referred to as a cloud service provider ("CSP").

The deployment models that are common in today's cloud computing environment include a private cloud (i.e., operated for an individual organization), a community cloud (i.e., shared by several organizations with common interests or requirements), a public cloud (i.e., available to large groups or the public), and a hybrid cloud (i.e., a combination of the various deployment models). The cloud service delivery models include those relating to: (i) software or business process management services (i.e., software as a service or "SaaS" and/or business process as a service or "BPaaS"), such as those relating to customer management, supply chain management, payroll), (ii) the creation of application systems and programs that operate on the CSP's hosted infrastructure (i.e., platform as a service or "PaaS"), or (iii) the CSP's provision of an infrastructure/data center (e.g., network, storage) (i.e., infrastructure as a service or "IaaS").

The paper notes that the key benefits of cloud computing may include, among other items: a reduced need for capital investment in IT, scalability of capacity, improved efficiency in resource allocation and use of information technology and related assets, enhanced speed of deployment, and environmental benefits (i.e., reduced power consumption).

**Overview of ERM Framework**

ERM is defined generally as a process for managing risk throughout the entire company in a manner that achieves the organization's objectives and provides a basis for defining the effectiveness of the company's risk management process. More specifically, ERM is defined as follows:

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."\(^2\)
The ERM framework is designed to assist an entity in achieving its organizational objectives. The COSO framework classifies organizational objectives according to the following categories:

- Strategic - high-level goals, aligned with and supporting its mission
- Operations - effective and efficient use of its resources
- Reporting - reliability of reporting
- Compliance - compliance with applicable laws, rules and regulations

The COSO ERM framework is intended to establish a best practice for assisting a company in making prudent risk management and governance decisions in evaluating cloud computing. The COSO ERM framework provides for a comprehensive evaluation based on consideration of the following factors:

- Internal Environment (i.e., the organization's risk management philosophy, risk appetite, integrity, ethic values, and operating environment);
- Objective Setting (i.e., evaluation of current or new objectives to support and align with the entity's mission and risk appetite);
- Event Identification (i.e., identifying events (either opportunities or risks) that may affect the achievement of objectives, including, external (e.g., regulatory, economic, social) and internal (e.g., company culture, financial position) factors);
- Risk Assessment (i.e., evaluate alterations to the company's risk profile due to changes in the likelihood and impact of risks);
- Risk Response (i.e., response to identified risks (e.g., avoidance, reduction, sharing, acceptance);
- Control Activities (i.e., policies and procedures to ensure risk responses are carried out);
- Information and Communication (i.e., identifying, capturing and communicating relevant information in a form and timeframe to enable company personnel to carry out their responsibilities); and
- Monitoring (i.e., assuring that the ERM program adequately addresses the relevant risks and facilitates the accomplishment of the organization's objectives).

**Focus of Key Risks**

The paper notes that companies may overlook key risks involved in cloud computing based on the lack of significant capital investment requirements and the relative ease and speed of adopting cloud computing. The paper notes that such key risks relating to cloud computing may include the following:

- Disruption to industry that may result from cloud computing transformation (e.g., eliminating barriers to entry, reducing need for capital, increased speed, etc.);
- Increased dependency and reliance on CSPs;
- Reduced and/or relinquishment of control to CSPs;
- Increased use of shared resources with other cloud tenants;
- Unauthorized cloud activity;
Identification of Legal/Regulatory Risks in Move to Cloud

The paper emphasizes the need to assure that proper due diligence is performed on key legal and regulatory issues that are triggered by a cloud computing assessment. More specifically, the paper notes that:

"The equation of big investment equals big impact is different with cloud computing, where a small investment can have a big impact. The need to expend a great amount of effort to analyze cloud computing risks and perform the related due diligence may be counterintuitive. Consequently, management could neglect to perform time-consuming steps such as confirming compliance with legal or regulatory requirements or evaluating the potential impact of the CSP on the organization's operation and risk profile."

The assessment of cloud computing requires an assessment of a broad range of legal and regulatory considerations relating to the company's current state environment as well as issues that may arise from the adoption and/or emergence of cloud computing or other significant technological changes. Certain factors to be addressed by a company in connection with the due diligence assessment regarding the potential conversion to, implementation of, and/or response to cloud computing may include, without limitation, assessment of the following items:

- Decreased transparency;
- Decreased portability to, or interoperability with, other solutions;
- Increased consolidation of data with other companies that may increase likelihood of cyber-attacks;
- Increased reliance on CSPs and other third-parties;
- Increased risk of data leakage;
- Increased risk of noncompliance; and
- Organizational changes.

- Laws, rules and regulations applicable to a company's IT operations, including the requirements imposed at the State and Federal levels and in each applicable foreign jurisdiction (e.g., Sarbanes Oxley Act of 2002 ("SOX"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), USA Patriot Act, the European Union Data Protection Directive, Malaysia's Personal Data Protection Act of 2010, and India's IT Amendments Act);
- Requirements imposed by accreditation bodies or other trade association standards applicable to company's operations (e.g., disaster preparedness, data set requirements, transaction processing requirements, benchmarks, quality reporting);
- Requirements set forth in a company's processes, policies, and internal controls designed to assure that IT operations operate in compliance with applicable laws, rules and regulations;
- Obligations under existing IT contractual arrangements with vendors (e.g., software, hardware, leasing, licensing, acquisition);
- Obligations relating to IT employees, independent contractors and other service providers (e.g., collective bargaining, independent contractors, outsourcing requirements);
- Nature of third-party and/or proprietary interests in intellectual property in IT, including, issues relating to the transfer, safeguard and/or exploitation of IT in a cloud environment;
- Application of IT in legal, contracting, compliance and other related functions;
Legal Counsel's Ongoing Role in Cloud Governance

Following the decision to convert to cloud computing, the legal office must continue to play a key role in the ERM approach. The paper notes that key cloud responsibilities for the company's legal counsel with respect to the adoption and/or ongoing governance of cloud activities may include the following:

- Use of IT to monitor and audit compliance with applicable legal and regulatory requirements; and
- Transfer, divestiture or other uses for existing IT assets;

Ensure that the organization's cloud activities comply with laws and regulations;

Monitor for new laws, and regulations that would impact the organization's cloud solution or its CSP and establish a plan for compliance;

Provide input on data classification policies and processes;

Negotiate/ review CSP contracts and ensure protection of the organization's interests and rights;

Understand the legal jurisdiction aspects of the organization's operations as they relate to using cloud services hosted in different countries;

The paper further emphasizes that the "significant ambiguity . . . in the international legal and regulatory environment" requires a comprehensive assessment of requirements in each jurisdiction that is impacted by the cloud operations. Such risk and related issues that need to be evaluated by legal counsel include those relating to:

- Location and movement of data storage and systems;
- Requirements imposed under domestic and foreign jurisdictions;
- Disclosure (e.g., subpoenas);
- Confiscation;
- Restrictions on access;
- Ability to separate and isolate data that is subject to restriction/confiscation; and
- Tax issues.

Conclusion

The approach described above in the ERM plan for Cloud Computing should be a critical part of any company's ERM process and crisis management plan for addressing the challenges and opportunities of cloud computing and other rapid changes in the delivery of technological solutions. In particular, the framework emphasizes the need for a company to ensure the appropriate consideration of legal risks in ERM, crisis management and related processes. Such an integration of legal and business processes in the approach to ERM, crisis management and related risk mitigation strategies represents a "best practice" that (i) is frequently lacking in the internal control environment and processes of many companies, and (ii) is necessary to provide additional assurances relating to, among other items, the appropriate:

- Assessment and response to risk arising under applicable laws, rules, regulations, accreditation guidelines and other standards applicable to IT and related functions;
- Up-front identification of experience, qualifications and other requirements of CSPs and other IT vendors during the
request for proposal ("RFP") process;

- Development of appropriate governance structures to clearly define roles and responsibilities necessary to administer the processes and/or supervise the performance of the CSP and/or other IT vendors;

- Development of appropriate policies, procedures and processes to assure that the processes will achieve the company’s objectives, including, those relating to compliance with applicable laws, rules and regulations;

- Development of training, education and communication programs for employees, management, Board members and other stakeholders;

- Negotiation and development of appropriate contractual terms and conditions required to safeguard the interests and reputation of the company, its customers and other stakeholders;

- Development and implementation of processes for effective ongoing monitoring and auditing to ensure the performance of the CSP and other IT vendors in accordance with the terms of agreements; and

- Development and implementation of any necessary corrective actions.

2 "Enterprise Risk Management — Integrated Framework, Executive Summary, COSO, September 2004
3 "Enterprise Risk Management — Integrated Framework, Executive Summary, COSO, September 2004

Your Key Contacts

Ross Docksey
Partner, Chicago
D +1 312 876 8171
ross.docksey@dentons.com

Jack (John) T. Gilbertson
Senior Counsel, Los Angeles
D +1 213 892 2913
john.gilbertson@dentons.com

Gary L. Goldberg
Senior Policy Director,
Washington, DC
D +1 202 408 6396
M +1 412 337 3191
gary.goldberg@dentons.com