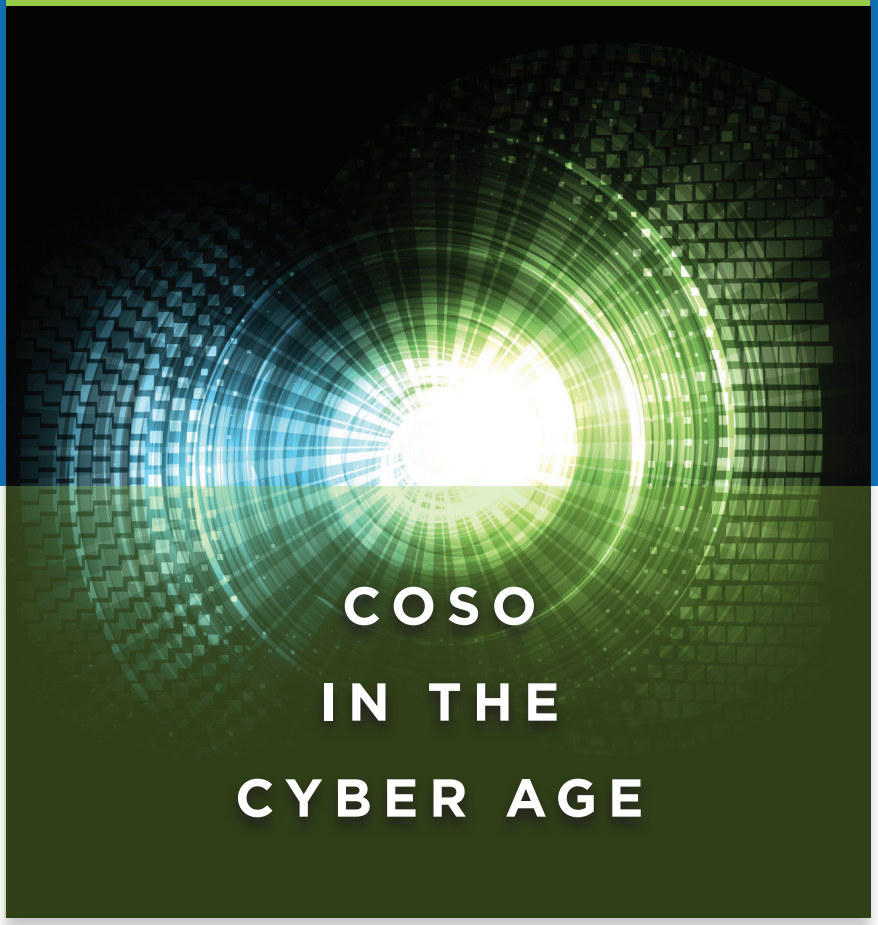
COSO

Committee of Sponsoring Organizations of the Treadway Commission

Governance and Internal Control



COSO IN THE CYBER AGE

By

Deloitte.

Mary E. Galligan | Kelly Rau

Authors

Deloitte & Touche LLP

Mary E. Galligan,
Director

Kelly Rau,
Senior Manager

Acknowledgements

We would like to recognize Jennifer Burns, Partner, Deloitte LLP and Sandy Herrygers, Partner, Deloitte & Touche LLP for their help and support in getting this article published.

COSO Board Members

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

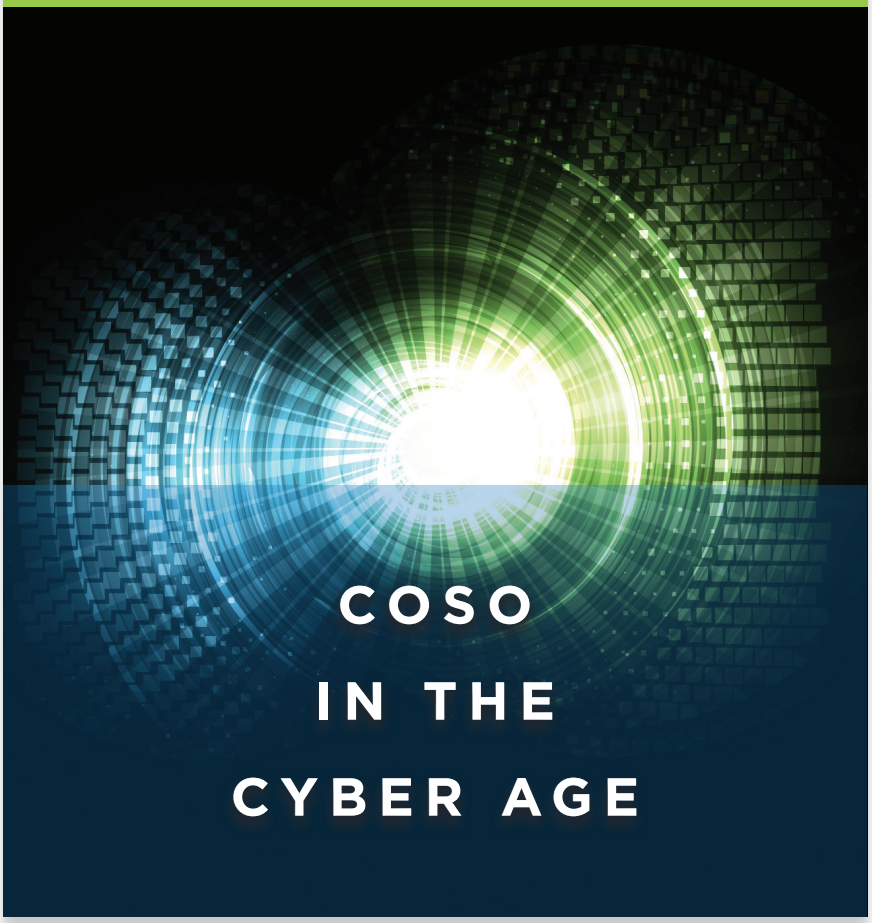
The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

COSO
Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org

Governance and Internal Control



COSO IN THE CYBER AGE

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

January 2015

1234567890 PIP 198765432

www.coso.org

Contents

[i] As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

The Evolution of Business in a Cyber-Driven World

As organizations consider how to address the evolving risks associated with cyber security, either the COSO Internal Control — Integrated Framework ("*2013 Framework*") or the Enterprise Risk Management Integrated Framework (2004) provide an effective and efficient approach to evaluate and manage such risks. Indeed, both frameworks provide structures that will lead organizations down similar paths of addressing cyber risk through the COSO lens. As companies have been focused on implementing the *2013 Framework*, in this paper, we leverage the *2013 Framework* to demonstrate how COSO can help manage cyber risks and controls.

In 1992, when the original COSO Internal Control — Integrated Framework ("*1992 Framework*") was released, businesses operated in a much different environment. For instance:

- There were less than 14 million Internet users worldwide in 1992, compared to nearly 3 billion today.[1, 2]
- America Online (AOL) for Microsoft DOS had been recently released.[3]
- Microsoft Internet Explorer did not exist.[4]
- Some of the most popular cell phones were "bag phones."[5]
- Telephone and fax were the predominant ways businesses communicated.

Over the past two decades, Information Technology (IT) has dramatically transformed the way businesses operate to the point where businesses exist in a primarily cyber-driven world. Customers' orders are now processed over electronic data interchanges on the Internet with little or no human intervention. Business processes are often outsourced to service providers, who are enabled by interconnected networks. More and more corporate personnel work remotely or from home, with little need to come into the office. Inventory is tracked in warehouses through the use of radio-frequency identification (RFID) tags. Online only banks exist, and nearly all banks offer Internet banking to customers.

As businesses and technology have evolved, so has the *2013 Framework*. One of the foundational drivers behind the update and release of the *2013 Framework* was the need to address how organizations use and rely on evolving technology for internal control purposes. The *2013 Framework* has been enhanced in many ways and incorporates how organizations should manage IT innovation considering:

- Globalization of markets and operations;
- Greater complexities of business processes;
- Demands and complexities in laws, rules, regulations, and standards;
- Use of, and reliance on, evolving technologies; and
- Expectations relating to preventing and detecting fraud.

Since the original *1992 Framework* was released, it is clear innovations in business have woven a rich complex fabric of connectivity through the Internet. However, the Internet was designed primarily for sharing information, not protecting it. On any given day, there are numerous media reports about significant cyber incidents. While cyber attacks in certain industries have dominated coverage in the news, all industries are susceptible to cyber attacks. Which data, systems, and assets are of value at any particular point in time depends on the cyber attacker's motives. As long as cyber incidents continue to have a negative impact on the financial well-being of victim companies and continue to draw additional regulatory scrutiny, cyber breaches will continue to be high profile events that draw a substantial amount of press.

---

[1] *The World Bank,* Data, Internet users (per 100 people), data.worldbank.org/indicator/IT.NET.USER P2?page=6&cid=GPD_44.

[2] *The World Bank*, Data, Population, total, data.worldbank.org/indicator/SP.POP.TOTL.

[3] *The Washington Post*, 25 years of AOL: A timeline, washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303551.html.

[4] *Encyclopedia Britannica,* Internet Explorer (IE), britannica.com/EBchecked/topic/291515/Internet-Explorer-IE.

[5] *Business Insider*, Justin Meyers, Watch The Incredible 70-Year Evolution Of The Cell Phone, businessinsider.com/complete-visual-history-of-cell-phones-2011-5?op=1#ixzz3FqJooiiX.

Further, IT will continue to transform how businesses operate in a global economy. This increasing digital reach, particularly considering how data is often shared by companies with external parties such as outsourced service providers, adds layers of complexity, volatility, and dependence on an infrastructure that is not fully within the control of the organization. Although trust relationships and controls may have been created and put in place between a company and external parties (e.g., service providers, vendors, and customers) to enable the sharing of information and electronic communications to conduct business operations, when a problem arises, the company is often held responsible for technology breaches outside of its perimeter. As companies continue to take advantage of new technologies and continue to use external parties to conduct operations, cyber attackers will take advantage of new vulnerabilities that allow information systems and controls to be exploited.

What is an "information system" according to the *2013 Framework*?

"An information system is the set of activities, involving people, processes, data and/or technology, which enable the organization to obtain, generate, use and communicate transactions and information to maintain accountability and measure and review the entity's performance or progress towards achievement of objectives."

While businesses use great caution when sharing information about their technology, both internally and externally, to protect their business operations, cyber attackers have the luxury of operating at the opposite end of the spectrum. They share information openly without boundaries, with little fear of legal repercussions, and often operate with a great deal of anonymity. Cyber attackers leverage technology to attack from virtually anywhere and to target virtually any kind of data.

The reality is that cyber risk is not something that can be avoided; instead, it must be managed.

Despite this far reaching cyber threat, it is clear that protecting all data is not possible, particularly considering how an organization's objectives, processes and technology will continue to evolve to support its operations. Each evolution creates an opportunity for exposure – and while evolution can be handled with care to minimize the opportunity for exposure it is impossible to be one hundred percent certain. Further, cyber attackers continue to evolve, finding new ways to exploit weaknesses. As a result, the reality is that cyber risk is not something that can be avoided; instead, it must be managed. Using a lens of what data is most important to an organization, management must invest in cost-justified security controls to protect its most important assets. By adopting a program to become secure, vigilant, and resilient, organizations can be more confident in their ability to reap the value of their strategic investments (refer to Deloitte's "*Secure.Vigilant.Resilient.*" approach in its document titled, *Changing the Game on Cyber Risk*).[6]

[6] Deloitte, *Changing the Game on Cyber Risk*, deloitte.com/view/en_US/us/Services/audit-enterprise-risk-services/cyber-risk/62ea116aaee44410VgnVCM2000003356f70aRCRD.htm.

In order to manage cyber risks in a secure, vigilant, resilient manner, organizations may view their cyber profile through the components of internal control. For example:

- **Control Environment** — Does the board of directors understand the organization's cyber risk profile and are they informed of how the organization is managing the evolving cyber risks management faces?
- **Risk Assessment** — Has the organization and its critical stakeholders evaluated its operations, reporting, and compliance objectives and gathered information to understand how cyber risk could impact such objectives?
- **Control Activities** — Has the entity developed control activities, including general control activities over technology, that enable the organization to manage cyber risk within the level of tolerance acceptable to the organization? Have such control activities been deployed through formalized policies and procedures?
- **Information and Communication** — Has the organization identified information requirements to manage internal control over cyber risk? Has the organization defined internal and external communication channels and protocols that support the functioning of internal control? How will the organization respond to, manage, and communicate a cyber risk event?
- **Monitoring Activities** — How will the organization select, develop, and perform evaluations to ascertain the design and operating effectiveness of internal controls that address cyber risks? When deficiencies are identified how are these deficiencies communicated and prioritized for corrective action? What is the organization doing to monitor their cyber risk profile?

Figure 1. The COSO Cube

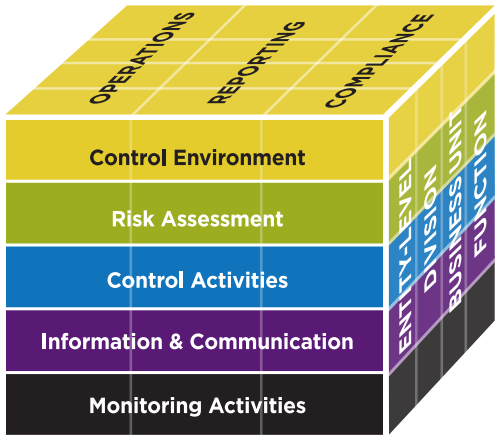


Figure 2. Internal Control Components and Related Principles

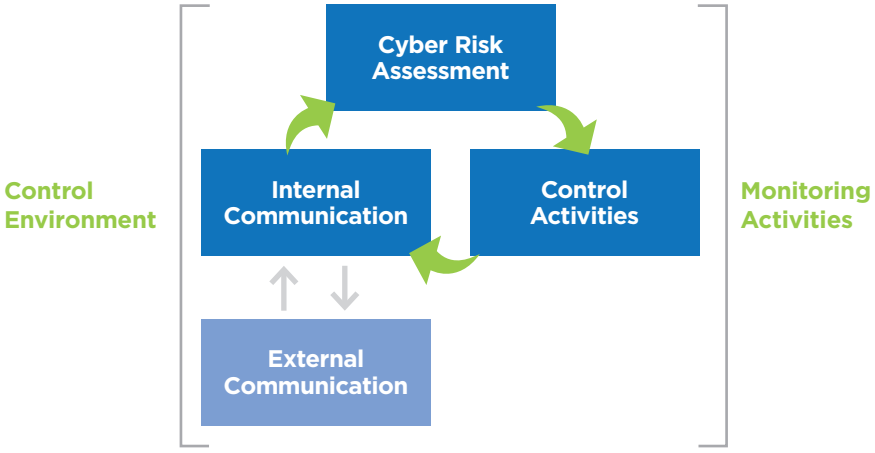
The following is a summary of the 17 internal control principles by internal control component as presented in the *2013 Framework*. (Please refer to the *2013 Framework* for the actual principles and related descriptions.)

Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring Activities
1. Demonstrates commitment to integrity and ethical values **2.** Exercises oversight responsibilities **3.** Establishes structure, authority, and responsibility **4.** Demonstrates commitment to competence **5.** Enforces Accountability	**6.** Specifies suitable objectives **7.** Identifies and analyzes risk **8.** Assesses fraud risk **9.** Identifies and analyzes significant change	**10.** Selects and develops control activities **11.** Selects and develops general controls over technology **12.** Deploys through policies and procedures	**13.** Uses relevant, quality information **14.** Communicates internally **15.** Communicates externally	**16.** Conducts ongoing and/or separate evaluations **17.** Evaluates and communicates deficiencies

When a company manages cyber risk through a COSO lens, it enables the board of directors and senior executives to better communicate their business objectives, their definition of critical information systems, and related risk tolerance levels. This enables others within the organization, including IT personnel, to perform a detailed cyber risk analysis by evaluating the information systems that are most likely to be targeted by attackers, the likely attack methods, and the points of intended exploitation. In turn, appropriate control activities can be put into place to address such risks.

As we discuss each of the internal control components in this paper, we will demonstrate how each component is interrelated with others and how the risk assessment process needs to be continuous and dynamic and incorporates information from both internal and external sources.

The Control Environment and Monitoring Activities components are foundational when considering cyber risk. In order for organizations to become secure, vigilant, and resilient, these components of internal control must be present and functioning — if not, it is likely that an organization will be unable to understand cyber risks sufficiently, deploy effectively designed control activities, and respond appropriately to address the cyber risks. As such, while the main focus of this white paper will be placed on the Risk Assessment, Control Activities, and Information and Communication components, we will discuss the considerations of Control Environment and Monitoring at the conclusion of the paper.



A COSO-focused Cyber Risk Assessment

Every organization faces a variety of cyber risks from external and internal sources. Cyber risks are evaluated against the possibility that an event will occur and adversely affect the achievement of the organization's objectives. Malicious actors, especially those motivated by financial gain, tend to operate on a cost/reward basis. The perpetrators of cyber attacks, and the motivations behind their attacks, generally fall into the following broad categories:

- **Nation-states and spies** — Hostile foreign nations who seek intellectual property and trade secrets for military and competitive advantage. Those that seek to steal national security secrets or intellectual property.
- **Organized criminals** — Perpetrators that use sophisticated tools to steal money or private and sensitive information about an entity's consumers (e.g., identity theft).
- **Terrorists** — Rogue groups or individuals who look to use the Internet to launch cyber attacks against critical infrastructure, including financial institutions.
- **Hacktivists** — Individuals or groups that want to make a social or political statement by stealing or publishing an organization's sensitive information.
- **Insiders** — Trusted individuals inside the organization who sell or share the organization's sensitive information.

While the results of the risk assessment will ultimately drive the allocation of entity resources against control activities which prevent, detect, and manage cyber risk, investments must also be directed at the risk assessment process itself. An organization has finite resources and its decisions to invest in control activities must be made upon relevant, quality information that prioritizes funding to the information systems that are the most critical to the entity.

An organization's cyber risk assessment should begin first by understanding what information systems are valuable to the organization. The value should be measured against the potential impact to the entity's objectives.

Principle 6

The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

The *2013 Framework* provides several points of focus, within Principle 6, that provide perspective to organizations on how to evaluate its objectives in a manner that could influence the cyber risk assessment process. These points of focus are defined under the following categories:

- Operations Objectives
- External Financial Reporting Objectives
- External Non-Financial Reporting Objectives
- Internal Reporting Objectives
- Compliance Objectives

Because the cyber risk assessment informs management's decisions about control activities deployed against information systems that support an entity's objectives, it is important that senior management and other critical stakeholders drive the risk assessment process to identify what must be protected in alignment with the entity's objectives. Many organizations do not spend enough time gaining an understanding of what information systems are truly critical to the organization; they also may have difficulty understanding where and how the information is stored. This can lead to attempts to protect everything, which leads to overprotecting certain information systems and under protecting others.

Placing a value on information systems requires a high degree of collaboration between business and IT stakeholders. Because organizations are not able to act on all risks, given the limited time, budget, and resources available, management should also determine the levels of risk tolerance acceptable to the organization and focus its efforts to protect the most critical information systems.

Principle 7

The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Principle 8

The organization considers the potential for fraud in assessing risks to the achievement of objectives.

As an output of the objectives identified as a result of applying Principle 6, an organization should have a clear understanding of the information systems critical to the achievement of its objectives. Applying Principle 7 and Principle 8 then take the risk assessment deeper and lead the organization to assess the severity and likelihood of cyber risk impacts. When led by senior management, through collaboration with business and IT stakeholders, an organization is positioned to evaluate the risks that could impact the achievement of its objectives across the entity.

To be effective in the risk assessment process, individuals who are involved must have an understanding of the organization's cyber risk profile. This involves understanding what information systems are valuable to perpetrators of cyber attacks, and understanding how these attacks are likely to occur. The costliest attacks tend to be the ones that are highly targeted at an organization for specific reasons. Organizations should be vigilant about understanding their particular cyber threat profile.

Being vigilant means establishing threat awareness throughout the organization and developing the capacity to detect patterns of behavior that may indicate, or even predict, compromise of critical assets. Organizations must incorporate this profile into their overall risk assessment process in order to understand where controls should be placed to keep those assets secure.

It is also important to apply an industry lens to cyber risks versus just looking broadly at cyber risks. The perpetrators of cyber attacks have unique objectives that differ between industry sectors. For example, in the retail sector, organized criminals are the most likely attackers, focused primarily on exploiting vulnerabilities in systems that contain information that can be used for profit (e.g., credit card data or Personally Identifiable Information (PII)). Alternatively, the oil and gas industry might be targeted by nation states with a motive to steal strategic data about future exploration sites. Chemical companies may find themselves targeted by hacktivists because of perceived environmental issues around their products.

Regardless of their motives, cyber attackers are relentless, sophisticated, and patient. They will stage attacks over time by gathering information that will expose weaknesses within the organization's information systems and internal controls. Through careful evaluation of the motives and likely attack methods and the techniques, tools, and processes (TTPs) the attackers may use, the organization can better anticipate what might occur and be in a position to design controls that are highly effective in minimizing the disruption of potential cyber attacks and keeping highly valued assets secure.

Principle 9

The organization identifies and assesses changes that could significantly impact the system of internal control.

Change is certain in any organization and should be anticipated in the performance of cyber risk assessments. The organization will evolve, which includes changes to its objectives, people, processes, and technologies. The cyber landscape will also change, which includes new perpetrators of cyber attacks along with new methods of exploitation. While cyber risk assessments are generally reflective of the current state of the organization, the process must be both dynamic and iterative and consider internal and external threat changes that could trigger the need to change how the organization manages its cyber risks.

Business and technology innovations are adopted by organizations in their quest for growth, innovation, and cost optimization. However, such innovations also create exposure to new cyber risks. For example, the continued adoption of Web, mobile, cloud, and social media technologies has increased the opportunity for exploitation by the perpetrators of cyber attacks. Similarly, outsourcing, offshoring, and third-party contracting have exposed organizations to potential cyber vulnerabilities that are ultimately outside of the organization's control. These trends have resulted in the development of cyber ecosystems that provide a broad attack surface for the perpetrators to exploit.

The assessment of changes that could have an impact on the system of internal control should include considerations regarding changes in personnel. Turnover of personnel at operational levels of the organization can have a significant impact on the organization's ability to effectively perform their control responsibilities that are designed to minimize the potential impacts of cyber attacks.

Risk assessments should be updated on a continuous basis to reflect changes that could impact an organization's deployment of cyber controls to protect its most critical information systems. As information is generated from the vigilant monitoring of the changing threat landscape and the risk assessment process, senior executives and other stakeholders must share and discuss this information to make informed decisions on how to best protect the organization against exposure to cyber risks.

Identifying and Implementing Control Activities that Address Cyber Risks

Control activities are the actions performed by individuals within the organization that help to ensure management's directives are followed in order to mitigate risks to the achievement of the objectives. Such control activities should be documented in policies to help ensure that control activities are carried out consistently across the organization.

As stated previously, cyber risks cannot be avoided, but such risks can be managed through careful design and implementation of appropriate controls. When an organization considers the likely attack methods and routes of exploitation (through the risk-assessment process), they are better positioned to minimize the potential impact that cyber breaches may have on its objectives. As organizations arrive at the reality that cyber breaches are inevitable, and have performed an appropriate cyber risk assessment, control structures should be deployed in a layered approach that prevent intruders from freely roaming the information systems after the initial layers of defense are compromised.

Because cyber risk exposure can come from many entry points, both internal and external to the organization, preventive and detective controls should be deployed to mitigate cyber risks. Well-designed preventive controls may stop attacks from being realized by keeping intruders outside of the organization's internal IT environment and keeping the information systems secure. Additional preventive controls may also be deployed within the internal IT environment to act as obstacles to slow the intruders. Even when exploits occur, the controls can allow an organization timely detection of breaches, which can enable management to take corrective actions and to assess potential damages as early as possible. After corrective actions are taken, it is important that management assess the root cause to improve its controls to prevent or detect similar exploits that may occur in the future.

CONTROL ACTIVITIES

Principle 10

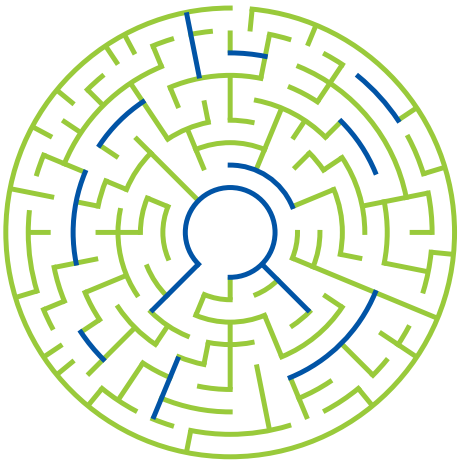
The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Principle 11

The organization selects and develops general control activities over technology to support the achievement of objectives.

Principle 12

The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.



What is the purpose of preventative and detective cyber controls?

Detective controls exist to identify that the threat has landed in our systems. Preventative controls exist to prevent the threat from coming in contact with the weakness.

In addition to preventative and detective controls, the control activities deployed to mitigate cyber risks should include a combination of general information technology controls ("GITC") along with other business controls. GITCs are the likely controls that will prevent or detect cyber breaches when they occur in order for the organization to be resilient. The detection of cyber events should trigger communications to inform others within the organization to take additional actions that may further mitigate risks. Because the risk assessment began with an understanding of the organization's objectives based on input from critical stakeholders, a map should exist in the most basic form to identify individuals that should be informed when cyber breaches occur.

While the *2013 Framework* provides principles and points of focus that direct organizations toward well-designed control activities, it was not intended to dictate the specific controls that should be implemented at organizations. Each organization is managed by different people with unique skills and experiences that drive the professional judgments that are applied to affect internal control. When evaluating if the organization has designed and implemented appropriate controls to mitigate cyber risks, it is helpful to compare control activities to standards and frameworks that are aligned with the management of cyber risks. Figure 3 below provides reference and background on the cyber-focused standards and frameworks that can provide additional assistance to organizations when evaluating the sufficiency of controls in order to be secure, vigilant, and resilient.

Figure 3. Cyber-focused Standards and Frameworks

COBIT
Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA that enables managers to bridge the gap between control requirements, technical issues and business risks.

ISO
The International Organization for Standardization developed the ISO 27000 series to address standards that enable organizations to implement processes and controls that support the principles of information security.

NIST
National Institute of Standards and Technology of the U.S. Department of Commerce released the first version of the Framework for Improving Critical Infrastructure Cybersecurity in February 2014. The framework builds on existing standards, guidelines, and practices to guide organizations in practices that reduce the potential impacts of cyber risks.

Generating and Communicating Relevant, Quality Information to Manage Cyber Risks and Controls

The Information and Communication component has three principles that focus organizations' efforts on (1) identifying relevant, quality information, (2) defining how information should be communicated internally and (3) defining how the organization should communicate with external parties. All other internal control components are dependent upon relevant, quality information that is supported by the Information and Communication component. While all of the points of focus should be considered when applying the *2013 Framework*, certain points of focus are critically important in the context of cyber risks and controls. These points of focus have been highlighted individually within this section.

Principle 13

The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

Identifies Information Requirements

The controls in place within an organization dictate the information requirements of the organization. This information could be in the form of reports, data used in control analysis, or overview diagrams that demonstrate a higher level view of the organization's extended business structure.

The identification of information requirements critical to internal control and the analysis of related cyber risks are interwoven with the risk-assessment process. For example, the information necessary to inform the cyber risk assessment would likely be structured in a cascading approach, using higher level information to inform more detailed risk assessment procedures.

Ultimately, the company needs to identify its information systems, determine their value, and protect them against cyber attacks through the deployment of control activities that are commensurate with the value of the information systems. To achieve this end result, business and IT stakeholders must initially arrive at a common understanding of the highest levels of the structure of the business, including outsourced service providers, and the related business objectives and sub-objectives that are important to the organization. Using this information as a base, an organization would then extend their risks assessment to further understand the information systems that may be exposed along with the likely attackers and attack methods. Once the risk assessment has been completed, this information is communicated to the organization to help ensure processes and controls have been designed to address such risks.

While this concept is easy to grasp, it is important to formally document information requirements (and the related risk analysis and response) to help ensure that processes and controls can be executed consistently with relevant, quality information in a manner that allows continuous refinement as people, process, and technology evolve along with the organization's objectives.

Processes Relevant Data into Information

Vigilant organizations in today's business environment can collect terabytes of log data related to their information systems. Security operations centers can generate an enormous number of alerts on a daily basis, ranging from tens of thousands to millions of events. To be vigilant with respect to cyber risks, it becomes critically important to transform raw data into meaningful, actionable information that has integrity.

Putting the data into context by identifying the patterns that signal potential cyber events is difficult for many organizations. With the massive volumes of data that are generated from various sources over days, weeks, and months, separating the signal from the noise can be extremely challenging. Further, cyber exploits are not often identified through the observation of a single event. More often the process of aggregating and correlating cyber data points from multiple sources over a period of time leads an organization to identify the pattern that escalates to action against detected cyber events. Without first transforming the raw data into actionable information that feeds into automated or manual controls, an organization cannot take proper action because the control is dependent upon the timely delivery of relevant, quality information that has integrity.

Captures Internal and External Sources of Data

The information requirements, as described above, drive the source of information that may be internal or external. While the primary source of information for cyber risk analysis and controls will be generated internally, it is also important for organizations to consider the need for external data. The following examples of external data sources are not all inclusive, but are likely relevant for most organizations.

- **Commercial / Industry Focused External Data:** Each company operates with an industry profile that drives similar patterns and trends from a cyber perspective. Companies within an industry have information systems that are similar in value and operate with similar technologies. This commonality affects the behavior of cyber attackers and the exploitation methods that are used. While sharing information externally must be handled with care, there can be significant benefits when such information is shared between trusted alliances or industry groups to discuss cyber event trends that can help to prevent or detect cyber risk events.
- **Government Agency External Data:** While government security clearance levels may be necessary to obtain access to certain information from governmental agencies, such information is extremely valuable when leveraged in the execution of internal controls against cyber risks. Many government agencies are supportive of improving processes and controls that defend organizations against the ever increasing cyber risk threats that evolve on a daily basis.
- **Outsourced Service Provider External Data:** Because organizations often outsource certain functions and processes to other service organizations, cyber event information from such organizations is necessary to have a complete view of cyber risks and controls. To enable the desired impact of outsourced operations, trust relationships are established that connect the information systems of both organizations. Still, both organizations have a vested interest in protecting their own unique information systems, and it is important to recognize that the need to share information is actually increased when cyber events threaten both entities and their business objectives. If a service provider or user organization experiences cyber events that may impact either organization's business operations, a level of transparency and collaboration to share such cyber event information can improve resilience in both organizations.

Maintains Quality Throughout Processing

The design of cyber control activities, which are dependent upon information, should consider the quality of the information used to execute such control activities. While information management policies should be established broadly at the organization, such policies should also be applied against cyber controls. There should be clear responsibility and accountability for the quality of the information that is supported by adhering to data governance expectations that protect data and information from unauthorized access or change.

An organization's ability to generate and use relevant, quality information to support the functioning of internal control is dependent on data governance. Educating and building consensus among stakeholders is essential for data governance programs—which can be made easier with an executive sponsor.[7] Once an effective data governance program is established and the organization practices discipline to maintain the program, information quality attributes (see Figure 4) will be realized. Information quality improves an organization's overall system of internal control and it also helps to improve cyber related internal controls.

Figure 4. Attributes of Quality Information
Excerpted from the *2013 Framework*

- **Accessible**— The information is easy to obtain by those who need it. Users know what information is available and where in the information system the information is accessible.
- **Correct**—The underlying data is accurate and complete. Information systems include validation checks that address accuracy and completeness, including necessary exception resolution procedures.
- **Current**—The data gathered is from current sources and is gathered at the frequency needed.
- **Protected**—Access to sensitive information is restricted to authorized personnel. Data categorization (e.g., confidential and top secret) supports information protection.
- **Retained**—Information is available over an extended period of time to support inquiries and inspections by external parties.
- **Sufficient**—There is enough information at the right level of detail relevant to information requirements. Extraneous data is eliminated to avoid inefficiency, misuse, or misinterpretation.
- **Timely**—The information is available from the information system when needed. Timely information helps with the early identification of events, trends, and issues.
- **Valid**—Information is obtained from authorized sources, gathered according to prescribed procedures, and represents events that actually occurred.
- **Verifiable**—Information is supported by evidence from the source. Management establishes information management policies with clear responsibility and accountability for the quality of the information.

[7] *Making Data Governance Programs More Effective*, deloitte.wsj.com/riskandcompliance/2014/08/04/good-riddance-to-bad-data-data-governance-gains-momentum/.

Principle 14

The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Communicates Internal Control Information

To All Personnel

Being secure, vigilant, and resilient is an organizational responsibility, where each individual plays a role in the protection of information systems. While certain personnel within the organization will have explicit roles to manage cyber risk and controls, each person within the organization must be vigilant when it comes to protecting information systems. An organization-wide communication plan should be developed and executed to raise the awareness of personnel within the organization about cyber risks and controls.

Such communications can help strengthen what can often be the weakest link of internal control – people – due to human nature. Think of the ramifications of human curiosity:

- What do people do when they receive an email from what is thought to be a trusted co-worker, customer, vendor, or other business partner? If the email looks to be official, a simple click of a hyperlink may begin the process of exploitation.
- What do people do if they find a USB drive lying on the floors? When they plug the USB drive into their computer to see who it might belong to, a door may be opened that exposes the company to an attacker's more sophisticated payload that was primed in the USB drive.

Characteristics of normal human behavior, such as human curiosity and trust of others, provide attackers with an opportunity to breakdown weaknesses of an entity's internal control structure. Communicating to all levels of the organization, on a regular basis heightens awareness of cyber security and reduces the likelihood that exploits aimed at entity personnel will be successful.

Communication plans may also incorporate different delivery strategies to maximize employee awareness of cyber risk and responsibility. Ongoing communications (e.g., live organizational meetings, entity wide messages) provide a mechanism of delivering relevant and timely updates to relevant entity personnel. Scheduled processes such as new employee onboarding or annual learning programs can also help to deliver similar updates within the organization.

To those Explicitly Responsible for Managing and Monitoring Cyber Risks and Controls

As noted in the Control Activities component earlier, management should select, develop, and deploy internal controls that are designed to protect information systems. Internal control information should be shared through internal channels to help management and entity personnel carry out their cyber control responsibilities across the organization.

Because of the complexities of the cyber landscape woven into the fabric of organizations, it is extremely important to maintain formal documentation on related cyber controls. Without formal documentation to support the expectations of internal control, an organization's ability to effectively manage cyber risks is dramatically reduced. An organization needs formal documentation to enable the efficient evaluation of the design and effectiveness of controls to protect the organization's information systems.

To the Board of Directors

Today, more than ever, boards of directors need to demonstrate their understanding of cyber trends that could impact the organization's ability to achieve its objectives. The board plays a fundamental role in being secure, vigilant, and resilient by understanding cyber risks, confirming preventative and detective controls are in place to manage such risks within a desired level of risk tolerance, and defining the expectation that appropriate response processes and procedures are established by management.

Effective communication between the board of directors and management, including senior executives and operational management, is critical for the board to exercise its internal control oversight responsibilities. To help enable effective communication at the board level, complex IT topics need to be translated into meaningful and actionable information.

While board membership is evolving towards inclusion of directors, or other sub-committee members, who have IT and/or cyber specialization, a majority of board members continue to have limited experience in these matters. This experience gap at the board level requires diligence in the interpretation and definition of information requirements that enable the board to exercise its oversight responsibilities.

In the definition of information requirements for the board, the organization may benefit by applying IT frameworks and standards that aim to translate technical IT topics into objectives that are meaningful for individuals that have either an IT or business background. Such frameworks and standards were mentioned earlier within the Control Activities component, which include COBIT[8] and ISO[9], and others that have been recently introduced such as the Cybersecurity Framework[10] issued by NIST.

While regularly scheduled communications at the board level may include updates on cyber topics, additional communication protocols should also be established to enable timely communications when major cyber emergencies are identified. As part of being resilient, timely communication to the board, with the best information available at the time, is important when major cyber risks are realized that could impact the achievement of the organization's objectives and could result in the need to communicate on such matters externally.

[8] Information Systems Audit and Control Association (ISACA), *COBIT*, isaca.org/cobit/pages/default.aspx.

[9] International Organization for Standardization (ISO), ISO/IEC 27001 - *Information security management*, iso.org/iso/home/standards/management-standards/iso27001.htm.

[10] National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, nist.gov/cyberframework/.

Principle 15

The organization communicates with external parties regarding matters affecting the functioning of internal control.

With External Parties

In the context of cyber security, the application of policies and standards is important to manage and control external communications. External communication may be relevant with shareholders, owners, customers, business partners, regulators, financial analysts, government entities, and other external parties. Two primary drivers exist for communication with external parties on cyber matters:

- To enable inbound communications to influence cyber risk assessment and controls.
- To facilitate outbound communications to inform external parties of cyber events, activities, or other circumstances that could affect how they interact with the entity.

Valuable information is brought into the organization through inbound communications. While management must validate the quality of such information, generally speaking, inbound communications provide value to inform cyber risk assessment and internal controls.

In contrast, outbound communications provide valuable information to external parties, as part of resilient activities. The communication of such information can potentially harm the communicating organization when not managed with proper care and controls. After information is released externally, the organization has limited influence on the control of such information and may not be able to influence how the information is used and potentially communicated to others beyond the intended audience.

With repercussions ranging from reputational damage, changes in stock price, the potential of lawsuits, causing potential harm to customers or other stakeholders, or even providing information that could lead to further exploits by attackers, it becomes clear that policies and standards are critically important to manage risk when balancing priorities to communicate externally while reducing the potential for negative impacts to the organization.

Control Environment and Monitoring Activities — Managing Cyber Risk is not possible Without Governance

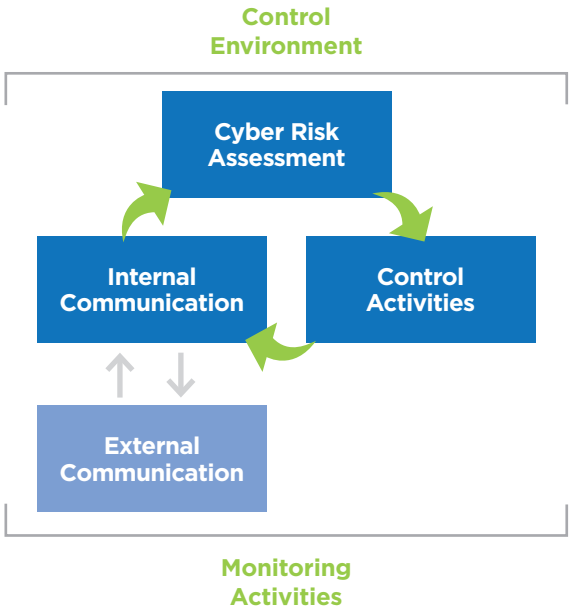
The Control Environment and Monitoring Activities internal control components are foundational for an organization to properly manage its cyber risk exposures.

As stated in the *2013 Framework*, "The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct."

Management and the board of directors have the authority and responsibility to set the top priorities of the company. If being secure, vigilant, and resilient is not defined as a priority and communicated within the organization, there is little hope that the organization will deploy sufficient resources to protect its information systems and to respond to cyber events appropriately.

The complexities of cyber risk can be a daunting challenge for management and the board of directors to get their arms around. To accomplish their responsibilities related to cyber risks, technical IT topics must be translated against an organization's objectives and business priorities. While some organizations may have internal professionals translate how IT may impact an organization's processes and objectives, many organizations require the assistance of qualified outside experts to help navigate strategy decisions that help them to become secure, vigilant, and resilient.

Assistance from qualified cyber risk specialists is critical to effectively prioritize the deployment of resources against cyber risks. Management and the board must be aware of and informed of the value of information systems that are aligned with the entity's objectives. With this information they can define their level of risk tolerance, and help ensure that adequate investments are directed towards the protection of information systems that are critical to the achievement of the organization's objectives.



As also stated in the *2013 Framework* with respect to Monitoring Activities, "Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component, is present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management and to the board."

Qualified cyber risk professionals are also critically important to the Monitoring Activities of the organization. Ongoing and separate evaluations help to evaluate the design and operating effectiveness of controls that are intended to reduce the potential exposure to cyber risks. In the event that professionals responsible for monitoring activities do not have strong cyber risk competencies, it is important to plan ahead to either develop these capabilities internally or to strategically address these needs through the assistance of outside experts.

As noted earlier, many companies' IT environments extend to other entities. In such cases, it is important to monitor cyber controls that operate at third parties or other outsourced service providers. If service auditor reports are not provided or do not sufficiently address cyber controls, a user organization should take steps to understand such controls in their efforts to remain secure and vigilant.

If leadership makes cyber risk management a priority and carefully assesses cyber controls through monitoring activities, the organization will be better positioned to deploy changes necessary to stay current against the evolution of cyber risks that can be controlled and/or predicted that could impact the entity's ability to achieve its objectives.

Equally important to the focus of leadership is the appropriate communication when deficiencies are identified. Proper communication of issues is essential to identifying the root cause of the situation, modifying appropriate control activities, and developing an appropriate remediation plan. In addition, to reinforce the vigilance of the organization, steps should be taken to ensure that control owners are held accountable to protect information systems.

Figure 5. Keys to Effective Control Environment and Monitoring of Cyber Risks Include:

- Clear tone from the top regarding the importance of protecting information systems
- A program of ongoing and separate evaluations to assess the design and operating effectiveness of controls that are intended to reduce potential cyber exposures
- Assistance and involvement of qualified cyber risk professionals
- Appropriate monitoring of cyber risk and controls related to outsourced service providers
- Proper and timely communication of cyber deficiencies
- Holding control owners accountable to help protect information systems

Conclusion

After consideration of cyber risk through the COSO lens, many organizations may reconsider how they can influence change to improve their controls that mitigate cyber risk impacts to the organization's objectives. If being secure, vigilant, and resilient has not been a priority for your organization, it will be eventually. If cyber risks are addressed by reactive management, the damage from a cyber attack could potentially be so severe that the organization could cease to exist and operate. Cyber risk will only continue to be more difficult to manage as time passes, technology evolves, and hackers become more sophisticated. Invest now and make cyber risk management a priority that receives similar attention as other objectives that are strategic to the organization.

Where to begin will depend on where an organization is today. The *2013 Framework* can be used to guide a transformation that supports an organization's efforts to design, evaluate, and maintain an environment of being secure, vigilant, and resilient in a cyber-driven world.

Appendix 1 – Key Questions to Ask

Are we focused on the right things?

Often said, but hard to execute. Understand how value is created in your organization, where your critical assets are, and how they are vulnerable to key threats. Practice defense in-depth.

Are we proactive or reactive?

Retrofitting for security is very expensive. Build it upfront in your management processes, applications and infrastructure. Identify if the proper controls are in place from a proactive and detective standpoint.

Are we adapting to change?

Policy reviews, assessments, and rehearsals of crisis response processes must be regularized to establish a culture of perpetual adaptation to the threat and risk landscape.

Do we have the right talent?

Quality over quantity. There is not enough talent to do everything in-house, so take a strategic approach to sourcing decisions.

Are we incentivizing openness and collaboration?

Build strong relationships with partners, law enforcement, regulators, and vendors. Foster internal cooperation across groups and functions, and ensure that people aren't hiding risks to protect themselves.

Can executive management articulate its cyber risks and explain its approach and response to such risks?

Having a well-defined process to identify risk, and respond to the risk makes it easier for executives to understand the organization's approach to cyber risks when having to explain the approach internally and to regulators.

Appendix 2 – Identifying Critical Information Systems

A key part of using the *2013 Framework* to manage cyber risk is to identify the information systems of value and conduct the risk assessments for those assets. Below is a high level approach to creating the information system inventory and risk assessment (as identified by COSO Principal 6). The result (output) will be an information asset inventory, gap analysis and prioritized controls to be implemented in your organization.

Identify Critical Information Systems

- Identify information categories based on business and organization objectives using the following as a guide:
  - > Corporate Policies
  - > Industry Standards (e.g., ISO)
  - > Regulatory Requirements
  - > Business Objectives
  - > Intellectual Property
  - > Financials
  - > Customer or Employee Data

Identify Where Information Systems Exist

- Identify how information is collected, used, transferred, stored and archived
- Identify business, system and application owners for information assets
- Create data flows to understand how information moves within business processes, systems and applications

Understand Risks Associated with Information Systems

- Analyze asset inventories and data flows to identify control risks
- Assess the likely perpetrators of cyber attacks and their likely attack methods
- Identify controls to address identified risks based on risk profile of the process, system or application

About the Authors

Mary E. Galligan, Director, Deloitte & Touche LLP

Mary Galligan is a Director in Deloitte's Cyber Risk Services practice. Mary advises senior executives on the crisis management challenges they face, in particular cyber risks. She helps companies develop and execute security programs to prevent and minimize the business impact of cyber threats. This includes board education, cyber war gaming, and other strategy efforts as the public and private sector collaboration around cybersecurity in the US begins to takes shape.

Mary joined Deloitte after retiring in 2013 from a distinguished career with the Federal Bureau of Investigations (FBI). Mary oversaw all FBI investigations into national security and criminal cyber intrusions in New York City, and advised numerous financial institutions, media entities and law firms during their high pressure situations. Her most recent position was with the New York Office as the Special Agent in Charge of Cyber and Special Operations, where she led the largest technical and physical surveillance operation in the FBI.

She gained significant crisis management experience as the supervisor over the FBI's investigation into the terrorist attacks on 9/11, as one of the On-Scene Commanders in Yemen after the bombing of the USS Cole, and as the Special Agent in Charge of Special Events and SWAT in New York City.

Mary held other leadership roles during her 25-year tenure with the FBI.

- First female Special Agent in Charge, New York, FBI
- Chief Inspector of the FBI
- Led a Director's Initiative on Risk-Based Management

Mary holds a bachelor's degree from Fordham University, Bronx, New York, a master's degree in psychology from the New School for Social Research, New York, New York, and an honorary doctorate of law from Marian University, Fond du Lac, Wisconsin.
She is an FBI-certified Crisis Negotiator and Crisis Manager.

Kelly Rau, Senior Manager, Deloitte & Touche LLP

Kelly Rau is a Senior Manager within Deloitte's Financial Statement & Internal Control Audit practice. Kelly joined Deloitte in 2002 and has extensive experience in assisting companies with a variety of internal control and information technology matters.
In his work with several Fortune 500 companies, Kelly has led internal control teams to understand, evaluate and improve the design and operating effectiveness of entity level, business cycle and information technology controls. Kelly also supports Deloitte's national office leadership in the oversight of the quality of IT audit services, including functioning as a consultation resource for IT and internal control related matters on Deloitte's largest and most complex integrated audits.

Kelly is a Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA) and holds both a master's of business administration and bachelor's degree in accounting from Central Michigan University.

About COSO

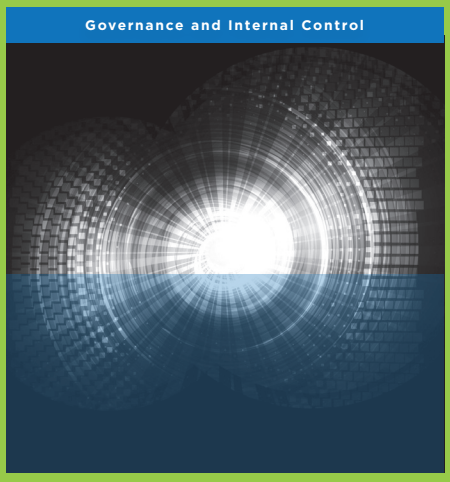
Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence. COSO's supporting organizations are the Institute of Internal Auditors (IIA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), and the Institute of Management Accountants (IMA).

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity.

Please see deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

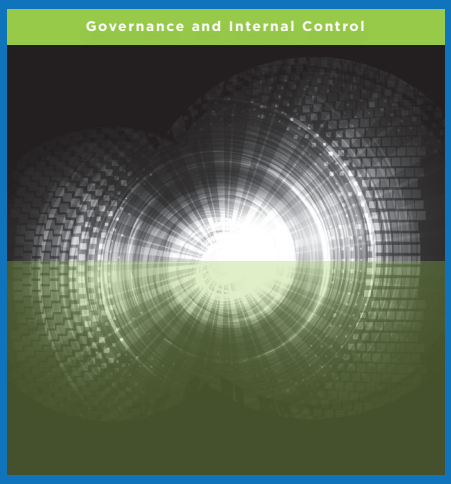
Member of Deloitte Touche Tohmatsu Limited.



COSO

Committee of Sponsoring Organizations
of the Treadway Commission

www.coso.org



COSO IN THE CYBER AGE

COSO

Committee of Sponsoring Organizations of the Treadway Commission

www.coso.org