COSO

Committee of Sponsoring Organizations of the Treadway Commission

Governance and Enterprise Risk Management

# MANAGING CYBER RISK IN A DIGITAL AGE

By

Deloitte.

**Mary E. Galligan | Sandy Herrygers | Kelly Rau**

## Authors

**Deloitte & Touche LLP**

**Mary E. Galligan**
Managing Director

**Sandy Herrygers**
Partner

**Kelly Rau**
Managing Director

## Acknowledgements

We would like to recognize Jeff Antonelli, Neha Awal, Lauren Bady, Brooks Castaneda, Bryan Czajka, Max Kadish, Michelle Rakovsky, Shikha Sharma, and Thomas Zimlich for their assistance in preparing the paper.

## 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

coso.org

Governance and Enterprise Risk Management

# MANAGING CYBER RISK IN A DIGITAL AGE

Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

November 2019

Design and production: Sergio Analco.

## Contents

# INTRODUCTION

The purpose of this guidance is to provide an overview for business executives and board members on cyber risk management through principles defined in the COSO Enterprise Risk Management Framework. This guidance provides context related to the fundamental concepts of cyber risk management techniques but is not intended to be a comprehensive guide to develop and implement technical strategies. Refer to the table below for additional context on the intended audience and use of this article.

| Audience | Intended Use |
|---|---|
| **Board of Directors**<br>**Audit Committee Members** | Understanding of the following topics to aid in oversight of management cyber processes:<br>• The need for board and executive involvement for an effective cyber risk management program<br>• How to leverage the COSO Enterprise Risk Management (ERM) Framework to govern the cyber security strategy, execution and monitoring program<br>• Key concepts and examples of cyber risk management strategies |
| **Executives**<br>(CEO, CIO, CRO, etc.) | Understanding of the following topics to aid executive direction of cyber risk management:<br>• How to leverage the COSO Enterprise Risk Management (ERM) Framework to manage cyber risk<br>• Overview of cyber risk considerations and mitigation techniques (e.g., risk appetite, risk prioritization)<br>• Illustrative examples of notable technical cyber security frameworks |
| **Cyber Practitioners** | Understanding of how cyber risk fits into an ERM approach |

## DIGITAL REVOLUTION

Cyber threats and attacks continue to grow in number and complexity – all while the business world grows increasingly connected and digital. As businesses and technology have evolved, so has the COSO Enterprise Risk Management (ERM) Framework, which was updated in 2017 and titled *Enterprise Risk Management – Integrating with Strategy and Performance* ("ERM Framework"). One of the foundational drivers behind the update of the ERM Framework was the need to address the evolution of risk management in the cyber age, and the need for organizations to improve their approach to managing cyber risk to meet the demands of an evolving business environment. The ERM Framework has been enhanced in many ways to highlight the importance of considering risk in both the strategy-setting process and in driving performance. The Framework:

- Provides greater insight into the value of risk management when setting and executing strategy.
- Enhances alignment between performance and risk management to improve the setting of performance targets and understanding the impact of risk on performance.
- Accommodates expectations for governance and oversight.
- Recognizes the globalization of markets and operations and the need to apply a common, albeit tailored, approach across geographies.
- Presents new ways to view risk to setting and achieving objectives in the context of greater business complexity.
- Expands reporting to address expectations for greater stakeholder transparency.
- Accommodates evolving technologies and the proliferation of data and analytics in supporting decision-making.
- Sets out core definitions, components, and principles for all levels of management involved in designing, implementing, and conducting ERM practices.[1]

### COSO 2017 ERM Framework Strategy


Source: COSO

It is clear that innovations in business and technology have woven a rich and complex fabric of connectivity, enhanced through the proliferation of the Internet, and more recently the emergence of readily available cloud-based solutions. However, as companies become more agile and innovative through the emergence of digital reach, new and ever-present vulnerabilities have emerged. On any given day, there are numerous media reports about significant cyber incidents. Organizations of all types and sizes 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 reputation and financial well-being of victim companies and continue to draw additional regulatory and legal scrutiny, cyber breaches will continue to be high profile events that draw a substantial amount of negative press.

> "
>
> 90% of organizations in North American that are engaged in Digital Transformation acknowledge their risk profiles have expanded due to their digital initiatives. Managing cybersecurity risks is the top risk management objective for decision makers at organizations engaged in Digital Transformation.
>
> Source: RSA Digital Risk Study, 2019, https://www.rsa.com/content/dam/en/white-paper/rsa-digital-risk-report-2019.pdf

The financial and identity well-being for victims of a cyber attack, including the organization's employees and consumers, continues to fuel the impact of cyber threats. Additionally, small businesses and local government agencies may be easier to target and exploit than large corporations with sophisticated intrusion prevention and detection systems, although the latter may be a more efficient source of disruption and illicit income. As a result, it is important for organizations to consider the cost-benefit of a cyber insurance policy in the event a data breach does occur to help transfer and mitigate the risk related to financial loss. However, it is equally important to understand the coverage and restrictions of the plan as there may be limitations, such as costs associated with reputational damage or refusal of the insurer to pay a claim due to issues with an organization's data classification policy, encryption standard, etc.

> "
>
> Digital incidents [are] now costing small businesses $200,000 on average, according to insurance carrier Hiscox, and 60% going out of business within six months of being victimized. The frequency with which these attacks are happening is also increasing, with more than half of all small businesses having suffered a breach within the last year and 4 in 10 having experienced multiple incidents.
>
> Source: Cyberattacks now cost small companies $200,000 on average, putting manyout of business, CNBC. https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

Further, digital transformation and IT will continue to evolve how organizations operate in a global landscape. This increasing digital reach, particularly considering how data is often shared by organizations 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 organizations 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 organization is often held responsible for technology breaches outside of its perimeter. Organization can even be 'guilty by association' in instances where their data is secure, but one of their vendors is affected by a breach. As companies continue to take advantage of new technologies (e.g. artificial intelligence, blockchain, cloud computing, machine learning, etc.) 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. According to a 2018 Ponemon Institute study entitled, "Data Risk in the Third-Party Ecosystem", 59% of companies have experienced a breach caused by a third party they use. Only 11% of companies in that study were confident they would even know if their sensitive data was lost or stolen by the third party. The level of dependency on third parties has effectively extended the scope of the enterprise and has become a significant contributor to information security breaches. Consequently, the ERM program must extend to managing cyber risk within the third-party ecosystem.

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 via the dark web, with little fear of legal repercussions, and often operate with a great deal of anonymity. Cyber attackers leverage technology and seek to exploit lapses in policy and security procedures to attack from virtually anywhere and to target virtually any kind of data. The attacker can be an inside or outside threat, and their motives can vary.

In addition to cyber-attacks, risks related to other cyber scenarios such as destructive malware, ransomware, and other vectors used to impair the confidentiality, availability, and integrity of information systems and data can substantially affect an organization's tangible and intangible assets. Despite this far reaching cyber threat, it is clear that protecting all data is not possible, particularly considering how an organization's strategy, processes and technology will continue to evolve to support its operations. Each evolution creates an opportunity for exposure. While evolution can be handled with care to minimize the opportunity for exposure, it is impossible to be certain all vulnerabilities have been addressed. Further, cyber attackers continue to evolve and find 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. Organizations should ensure they have an understanding of all data that is collected, how it is collected, where that data is stored, and then focus on their most important data to deploy the appropriate security controls and other risk mitigation techniques to protect the organization's informational assets, brand and reputation, supply chains, etc.

Organizations may view their cyber risk profile through the following components of risk management as per the COSO ERM Framework[1]:

## Risk Management Components


Source: COSO

- **Governance and Culture:** Governance and culture together form a basis for all other components of ERM. Governance sets the entity's tone, reinforcing the importance of cyber vigilance and establishing oversight responsibilities for the entity.

- **Strategy and Objective-Setting:** Cyber risk management is integrated into the entity's strategic plan through the process of setting strategy and business objectives. With an understanding of business context, the organization can gain insight into internal and external factors and their effect on risk. An organization sets its cyber risk appetite in conjunction with strategy-setting. The business objectives allow strategy to be put into practice and shape the entity's day-to-day operations and priorities.

- **Performance:** An organization identifies and assesses risks that may affect an entity's ability to achieve its strategy and business objectives. As part of that pursuit, the organization identifies and assesses cyber risks that may affect the achievement of that strategy and business objectives. It prioritizes risks according to their severity and considering the entity's cyber risk appetite. The organization then selects risk responses and monitors performance for change. In this way, it develops a portfolio view of the amount of risk the entity has assumed in the pursuit of its strategy and entity-level business objectives.

- **Review and Revision:** By reviewing cyber risk management capabilities and practices, and the entity's performance relative to its targets, an organization can consider how well the cyber risk management capabilities and practices have increased value over time and will continue to drive value in light of substantial changes.

- **Information, Communication, and Reporting:** Communication is the continual, iterative process of obtaining information and sharing it throughout the entity. Management uses relevant information from both internal and external sources to support cyber risk management. The organization leverages information systems to capture, process, and manage data and information. By using information that applies to all components, the organization reports on risk, culture, and performance.

While organizations should customize their approach to managing cyber risks based on their unique business context, the ERM Framework provides a foundation for designing such an approach. The ERM Framework's 20 principles are described below, with discussion tailored to how these principles can address the inherent exposure to cyber risks.

## GOVERNANCE & CULTURE

| Principle | Description |
|---|---|
| 1. Exercises Board Risk Oversight | The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives. |
| 2. Establishes Operating Structures | The organization establishes operating structures in the pursuit of strategy and business objectives. |
| 3. Defines Desired Culture | The organization defines the desired behaviors that characterize the entity's desired culture. |
| 4. Demonstrates Commitment to Core Values | The organization demonstrates a commitment to the entity's core values. |
| 5. Attracts, Develops and Retains Capable Individuals | The organization is committed to building human capital in alignment with the strategy and business objective. |

As cyber threat activity increases in occurrence, complexity, and destructiveness, organizations face a greater risk to achieving strategy and business objectives. The impacts of a breach can involve data loss, business disruption, brand and reputation damage, and possible regulatory and legal implications. As such, the board of directors must contemplate cyber risk as part of the broader enterprise risk and not view it as only an IT matter. "For nearly half of responding organizations (49%), cybersecurity is on the board's agenda, at least quarterly, according to Deloitte's 2019 Future of Cyber Survey."[2]

> "For nearly half of organizations (49%), cybersecurity is on the board's agenda, at least quarterly.
>
> Source: Deloitte's 2019 Future of Cyber Survey, in conjunction with Wakefield Research, of 500 C-level executives who oversee cybersecurity at companies with at least $500 million in annual revenue including 100 CISOs, 100 CSOs, 100 CTOs, 100 CIOs, and 100 CROs between January 9, 2019, and January 25, 2019, using an online survey.

It is imperative that the board of directors develop or acquire cyber security expertise or advisors with relevant expertise. "The percentage of public companies that have appointed technology-focused board members has grown over the last six years from 10 percent to 17 percent."[3]

> "The percentage of public companies that have appointed technology-focused board members has grown over the last six years from 10 percent to 17 percent.
>
> Source: Khalid Kark, Caroline Brown, Jason Lewris, Bridging the boardroom's technology gap, Deloitte University Press, June 29, 2017.

While this is a significant increase, there is still a great opportunity to grow this number. The fast-evolving cyber threat landscape demands that the board of directors increase cyber competencies to understand cyber risks, evaluate the organization's cyber program and initiatives, and evaluate the extent that the cyber risks facing the organization are being addressed. For example, if the composition of a board of directors lacks cyber risk knowledge and experience, they can leverage independent advisors to bring industry-wide perspective on cyber trends. Board governance of cyber risk includes oversight of the organization's cyber security strategy, execution and monitoring program. This includes ensuring relevant and appropriate public disclosure of cyber risk factors and/or a material cyber security breach. For example, the board may seek to understand the entity's cyber security posture in comparison to other entities in the same industry. And, given the volume of publicly disclosed risk factors and cyber security breaches, it is possible for the board to oversee the entity's cyber disclosures in comparison to industry peers as well.

Due to the pervasive nature of cyber risk, it is important that organizations approach cyber security from an ERM perspective. Such an integrated management approach to dealing with cyber risk involves creation of a cyber risk management team, generally led by the chief information officer or chief information security officer, and is composed of members of senior management such as the chief financial officer, chief risk officer, general counsel, or chief operating officer. The team should comprise cross-departmental and cross-functional representation that assesses enterprise wide cyber risks based on a framework, evaluates the risks of cyber threats, develops an enterprise wide cyber security management plan, and develops a budget to mitigate cyber risks. The cyber risk management team should report to the board of directors on the impact of cyber threats and the associated risk management initiatives. The organization's chief audit executive should also be either part of this team or an independent advisor to the team.

Core traits of companies that have already reached the highest maturity level as defined by the National Institute of Standards and Technology (NIST)[4], include:

- Securing the involvement of senior leadership, both top executives and the board;
- Raising cybersecurity's profile within the organization beyond the information technology (IT) department to give the security function higher-level attention and greater clout; and
- Aligning cybersecurity efforts more closely with the company's business strategy.

The cyber security culture of an organization, its security awareness, and related desired employee behaviors starts with the board of directors and management and is inclusive of all employees. The cyber security culture should be embedded in the organization's culture. Organizations with a strong culture focused on cyber security awareness, training, and data loss prevention may reduce the susceptibility to phishing attempts, social engineering, and other forms of cyber-attacks. Organizational culture is defined as "'the way things work around here…' it includes the values, beliefs, behaviors, artifacts, and reward systems that influence people's behavior on a day-to-day basis. It is driven by top leadership and becomes deeply embedded in the company through a myriad of processes, reward systems, and behaviors."[5]

> "While cyber and IT issues have grown to represent nearly 20 percent of the average internal audit plan, individually these key issues continue to lag behind others considered lower risks by boards, such as operational, financial, reporting, and compliance/regulatory.
>
> Source: IIA 2019 North American Pulse of Internal Audit Survey.

An organization's cyber risk management program needs to be consistent with the entity's core values as established by the board of directors and senior management. The program's policies, standards, employee expectations, accountability, and all related communications should demonstrate support for the organization's core values. For example, management should seek to build the trust of employees getting them to buy into the importance of cyber vigilance rather than trying to coerce the desired behaviors. Senior leadership should also exhibit the desired cyber behaviors and habits to set the correct tone.

Organizations with an effective cyber culture have buy-in and involvement of senior leadership to model the culture and desired behaviors. Investment in ongoing cyber training initiatives and periodic monitoring of employee views on cyber risk should promote employee awareness of their role in cyber security and employee behavior and habits outlined in the cyber security program. For example, many organizations have implemented training programs that test an end user's ability to avoid a phishing attack. If the end user clicks on a fake phishing link, they are reminded of the need for diligence in evaluating unusual emails. Other organizations share videos with employees of bad end user security practices to educate users and many also use software to identify external email addresses and emails with potential inappropriate links in them and filter them out as part of their email filtering program. In addition, as part of training, employees should know how and where to report a potential cyber issue and be encouraged to do so.

### Organization's Cyber Risk Management Program




Cyber threats continue to evolve at faster rates, get more complex, and involve new exploit arsenals. Involvement of qualified cyber risk professionals is critical to effectively assessing cyber risks for an organization, implementing risk mitigation, and monitoring the effectiveness of the cyber security program. Some organizations may have in-house professionals with the appropriate qualifications, but others may require the assistance of qualified outside experts. For example, certain organizations have established minimum expectations for cyber competence in their information security team, such as requiring relevant certifications (e.g., Certified Information Security Services Professional ("CISSP") credentials). Additionally, expanded skills and/or training for newly adopted technologies are essential to manage risk resulting from organizations, including technical resources, not understanding risks related to the misconfiguration of new architectures and platforms. And, where unique skillsets are needed, an outside firm may be engaged to assist with the cyber risk assessment, implementation of resilience measures, and/or periodic assessments of the effectiveness of the program. Further, if an organization experiences a significant cyber security incident or breach, outside expert assistance may be needed to perform forensic or investigative work.

Governance should also include a system for data management and retirement of legacy systems. A common lowest point of failure is a legacy system that stays on a network with vulnerabilities such as default passwords or overly generous access allowing users to access the hardware and data well after it should be decommissioned or destroyed. This is also a risk for dark data that few IT staff remember exists on older storage devices and databases that may have a higher likelihood of exploitation.

Governance & Culture is a key foundational component to managing cyber risk and should drive segregation of duties in job responsibilities and system access and the execution of a business strategy that incorporates multiple lines of defense across the organization.

## STRATEGY & OBJECTIVE SETTING

| Principle | Description |
|---|---|
| **6. Analyzes Business Context** | The organization considers potential effects of business context on risk profile. |
| **7. Defines Risk Appetite** | The organization defines risk appetite in the context of creating, preserving, and realizing value. |
| **8. Evaluates Alternative Strategies** | The organization evaluates alternative strategies and potential impact on risk profile. |
| **9. Formulates Business Objectives** | The organization considers risk while establishing the business objectives at various levels that align and support strategy. |

"Business context" refers to the trends, relationships, and other factors that influence an organization's current and future strategy and business objectives. In today's fast changing environment, the current cyber environment needs to be understood for companies to adapt to the everchanging landscape. To do this, the periodic review of strategy and business objectives should consider the information and technology that is critical to accomplishing the business objectives of the organization both now and in the future state.

> By 2021, cybercrime damage is expected to hit $6 trillion annually—the equivalent of almost 10% of the world's economy.
>
> Source: https://deloitte.wsj.com/cio/2019/07/11/cyber-incidents-and-breaches-the-data-dilemma/

As an example, a manufacturer may currently deliver its business objectives related to shareholder value through revenue generated from traditional retail channels. In this current state, the information and systems related to manufacturing and shipping of business to business orders are the most critical assets tied to shareholder value. Looking toward the future in the organization's multi-year strategic plan, management plans to significantly invest and grow their direct to consumer revenue channel. While the traditional operations will continue to support the overall business objectives, new information and systems must be contemplated in the technology and marketing roadmaps to enable them to accomplish future state business objectives.

As change occurs, the organization must consider the new cyber risks that are present with respect to new systems, the ecommerce footprint on the internet, mobile application security, and protection of information and integrity of consumer loyalty programs. Cyber security must be considered as business context evolves in the constantly changing operating environment of the organization.

Companies need to stay aware of current risks, trends, and influencers in the cyber space. By 2021, cybercrime damage is expected to hit $6 trillion annually—the equivalent of almost 10% of the world's economy.[6] Cyber criminals are finding new and innovative ways to attack companies. Typically, once a method of attack is shown to work, that same method is used by multiple cyber criminals. Based on responses to Deloitte's 2019 Future of Cyber Survey, almost all C-level executives surveyed (95%) admit their companies have experienced a wide range of cyberattacks, with serious effects on their revenue, reputations, and leadership stability. Additionally, 90% of organizations experienced at least one disclosure of sensitive production data within the past year while 41% experienced more than 5 instances.

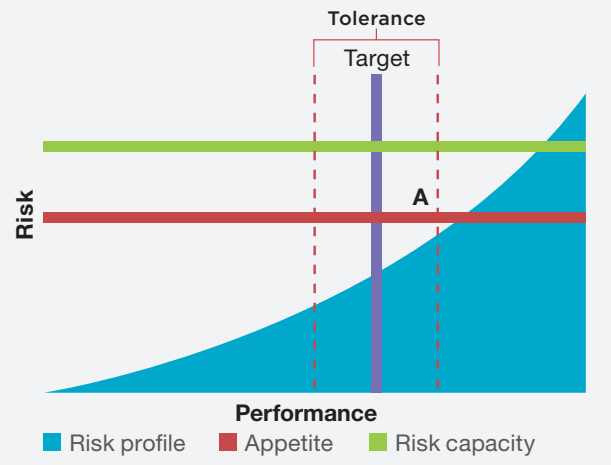
Defining risk appetite and the appropriate balance of cyber risk vs. reward is something that every organization must consider. One aspect of risk appetite that is increasingly important to digital initiatives is the cost-benefit of not adopting advanced technology or expanding technical capabilities. Organizations are finding they have to move faster, deploy more advanced technologies, and therefore their risk appetite may need to be adjusted in certain circumstances beyond what the organization has traditionally accepted in existing business operations. As organizations work to evaluate the current cyber environment, management needs to evaluate the extent they plan to deploy their cyber program. As part of this process, organizations need to inventory critical assets, identify the risk and determine where cyber vulnerabilities exist.

From that analysis, management can then better determine which business units, locations, and technology platforms need to be incorporated into the program and to what degree. These factors can help organizations develop and continuously update their risk appetite as it relates to cyber security. For example, a company highly dependent on technology with a significant ecommerce footprint may have a lower cyber risk appetite for the technology and information related to their ecommerce business operations. Likewise, the same company may have a higher risk appetite for information and systems that are not core to accomplishing their primary business objectives. Once the organization's risk appetite for cyber security has been determined, this needs to be communicated by management to all key stakeholders of the business and ultimately monitored through oversight by the board of directors. As an organization's risk appetite may change, it is important to consider how to manage risk appetite decisions when change is expected and when it occurs. Building off of the previous example of the manufacturing entity with the traditional retail channel with change anticipated in the direct to consumer space, the revenue generation may be small in the early expansion to direct to consumer marketing. However, the investments to get to that stage might be significant and the reputational risks in the market are likely to be high. In this situation, the risk appetite for this particular business expansion may be low and the organization may choose to invest more resources towards cyber security and resiliency based on the significance of the planned future revenue in support of the business objectives of the organization.

Once the cyber security risk appetite is defined, management identifies a security model to help govern its cyber risk management program. When determining what cyber security model management will implement, several factors need to be evaluated in conjunction with identifying the right cyber strategy for the organization. Some of these factors include capital, resources, and technologies. Several cybersecurity frameworks such as the NIST's Cybersecurity Framework,[7] the International Organization for Standardization (ISO)'s ISO 27001/2,[8] and the AICPA Cybersecurity Risk Management Reporting Framework[9] have been developed to help organizations establish and report on the effectiveness of their cyber security program. Organizations must determine which cybersecurity framework is the best fit based upon their business operations, current control structure, and other various factors. Refer to **Appendix** for illustrative examples of cybersecurity frameworks.

It is key for management to align the cyber security program to the business objectives and set targets. Methods such as The Open Group's FAIR (Factor Analysis of Information Risk) can be leveraged to quantify risk and derive values for risk tolerance evaluation. Certain tolerances or acceptable variations in performance may be established to help ensure the risk management program operates within the boundaries that are defined and understood, including a defined maximum tolerance threshold based on management's risk appetite ("A" in the Risk Tolerance Threshold below). For non-critical assets, management might determine a less aggressive cyber security model than for critical assets. Additionally, re-evaluation of the cyber security program is important given the dynamic movement in the cyber space. Upon evaluation, if targets are not met and established tolerances are exceeded, the cyber security risk appetite and/or cyber governance model may need to be revisited.

### Risk Tolerance Threshold




Source: COSO

Strategy & Objective setting are key to managing cyber risk and they must be integrated with overall strategy and business objectives.

## PERFORMANCE

| Principle | Description |
|---|---|
| 10. Identifies Risk | The organization identifies risk that impacts the performance of strategy and business objectives. |
| 11. Assesses Severity of Risk | The organization assesses the severity of risk. |
| 12. Prioritizes Risk | The organization prioritizes risks as a basis for selecting responses to risks. |
| 13. Implements Risk Responses | The organization identifies and selects risk responses. |
| 14. Develops Portfolio View | The organization develops and evaluates a portfolio view of risk. |

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 (e.g., 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 should ultimately drive the allocation of entity's resources toward risk management responses designed to 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 these responses must be made upon relevant, quality information that prioritizes funding to the information systems that are the most critical to the entity.

### Organization's Cyber Risk Assessment Program

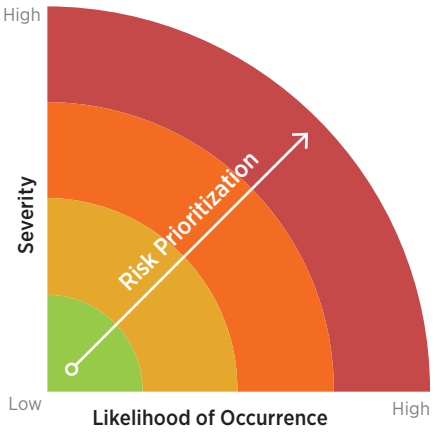



An organization's cyber risk assessment should begin first by understanding what information and systems are valuable to the organization. The value should be measured against the potential impact to the entity's objectives (including the potential impact of failed legal or regulatory compliance, which can have an indirect effect on accomplishing business objectives). For example, companies in various industries (e.g., financial services, technology, healthcare) may be a prime target for cyber crime given their assets and the highly automated nature of business transactions, processes, and systems.

Because the cyber risk assessment informs management's decisions about how to deploy risk responses toward 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 may result in 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.

### Risk Assessment Prioritization






As an output of Principles 10 and 11, an organization should have a clear understanding of the information systems critical to the achievement of its objectives. Then, applying Principle 12, risk assessment is taken deeper as the organization assesses and prioritizes risks in relation to the severity and likelihood of cyber risk events and outcomes. 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.

During this stage of the risk assessment process, 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.

Through careful evaluation of the motives and likely attack methods and the techniques, tools, and processes the attackers may use, the organization can better anticipate what might occur and be in a position to design controls and other risk responses that are highly effective in minimizing the disruption of potential cyber attacks and keeping highly valued assets secure.

The portfolio view of risks should be updated on a continuous basis to reflect changes that could impact an organization's deployment of cyber risk management activities 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.

Risk responses may come in the form of accepting risk, where the organization can tolerate the outcomes, transferring risk when others can manage the risks more effectively or efficiently, or acting to mitigate or reduce such risks. Because the risk assessment drives these decisions, it is important to consider that such responses are appropriate for the organization's risk appetite. When decisions are made to act on such risks, an organization normally deploys control activities. Control activities are the actions performed by individuals within the organization that help to ensure management's directives are followed 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 responses and recovery processes. 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 accept 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, or detecting when an intrusion has occurred. Additionally, the importance of an efficient and robust recovery process is critical, but the extent may vary depending on the type of attack and level of exposure. For example, the recovery process is critical in a large scale ransomware attack that restricts access to an organization's informational assets until the ransom is paid for the "key" to access the data, which may cost hundreds of thousands of dollars to be paid in crypto-currency that is not recoverable even if the "key" is not provided or does not remove the ransomware. This type of attack may require re-imaging and restoring each device from the most recent data backup to restart operations and avoid the risk of paying the ransom fee and becoming a consistent target for attackers seeking additional payments. However, the recovery process may not be as critical in an incident where malware was installed on one employee's laptop computer and removed from the organization's network before impacting other devices.

Because cyber risk exposure can come from many entry points, both internal and external to the organization, both 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 (e.g., a honeypot system) may also be deployed within the internal IT environment to act as obstacles to slow the intruders. Even when exploits occur, detective 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.

Ultimately, organizations must adopt, and continuously update, comprehensive policies and deliver training in disaster recovery, business continuity, data security, crisis management, and public relations to effectively respond to and recover from cyber attacks. As a result, having a robust process to identify, prioritize, and respond to risks to the achievement of strategy and business objectives is critical to delivering performance.

## REVIEW & REVISION

| Principle | Description |
|---|---|
| **15. Assesses Substantial Change** | The organization identifies and assesses changes that may substantially affect strategy and business objectives. |
| **16. Reviews Risk and Performance** | The organization reviews entity performance and considers risk. |
| **17. Pursues Improvement in Enterprise Risk Management** | The organization pursues improvement of enterprise risk management. |

Rapid evolution in information technology, adoption of that technology by employees, global supply chains, and permeation of industrial Internet of Things in businesses are increasing the threat of cyber attacks to organizations. A successful cyber attack can have significant financial and reputational impact on an organization. To mitigate the risk of a successful cyber attack, organizations should develop processes to identify and assess how a significant change would influence strategy, business objectives, and risk appetite.

For example, a manufacturing organization planning to implement smart factory solutions, which use artificial intelligence and networked sensors, would need to review its existing operational, financial, and technical strategies to address the cyber security risks that arise. The review could entail a cost and benefit analysis of developing a robust cyber risk management program, hiring qualified cyber risk professionals or re-training existing employees, or performing ongoing evaluations of new security vulnerabilities. Additionally, the organization would need to manage its external environment such as impact to its vendors, customers, and regulators, including communication in case of a successful cyber breach.

Cyber risk assessment processes are iterative as changes occur in an organization's internal and external environment. The organization must evaluate each change to determine its impact on the enterprise and determine how to best manage the cyber risk.

Organizations should constantly assess their cyber security risk assessment initiatives to determine if they are able to identify and mitigate the risk associated with these threats and potential attacks. To perform ongoing assessments, management must clearly articulate the goals, indicators for measuring performance, and consequences of missing targets. The consequences of missing targets should be proportional to the risk and the impact of a potential breach. Subsequently, assurance on control effectiveness related to cyber risk (i.e. how risk controls are periodically monitored and tested) can be performed by the internal audit department or by an external auditor for independent reporting purposes. For example, the AICPA has released guidance for the "System and Organization Controls ("SOC") for Cybersecurity engagement, through which a CPA reports on an organizations' enterprise-wide cybersecurity risk management program. This information can help senior management, boards of directors, analysts, investors and business partners gain a better understanding of organizations' efforts"[10] and provide an independent opinion on the effectiveness and maturity of an organization's cybersecurity program.

Consider, for example, that management determined phishing e-mails to be high risk to the organization. Management implemented an employee-training program to ensure employees were aware of the risk. The goal was also to ensure that 100% of employees would not click on phishing e-mails. If, after implementing this program, the organization still had measurable problems with phishing, they need to revisit the program and make revisions, such as implementing software to scan for phishing-like emails in addition to employee training.

For organizations looking to evolve and implement new technologies, cyber risk avoidance may not be an effective strategy. Management must therefore implement effective cyber risk strategies to become more vigilant (e.g., comprehensively monitor the extensive threat landscape). Feedback from comprehensive risk monitoring should feed into the risk assessment process.

New technological advances, feedback from the cyber security assessment, organizational changes, review of risk appetite, improved communication processes, and comparisons to other industries and competitors are examples of inputs that can help improve the risk management process. For example, a manufacturing organization planning to implement smart factory solutions, which use artificial intelligence and networked sensors, may not have considered the impact of cyber breaches in connected devices as part of prior risk assessments. However, changes in technology and changes in business objectives require improvements to the risk assessment processes to factor in new cyber risks.

Organizations must operationalize governance processes to capture and evaluate potential changes that may alter their cyber risk profile. This includes—at a minimum—capturing prospective new and changing products and services, information technology and evolving digital strategies, business processes, mergers, acquisitions, and reorganizations, and laws and regulations. Each of these items must be evaluated by qualified key stakeholders operating within a broad cyber risk management program. In addition, the importance of key indicators and control testing in monitoring for changes in the organization's cyber risk profile must remain a top priority.

The Review & Revision component is key as the constantly evolving cyber world disruption and digitization continue to drive the need for changes and enhancements to cyber risk management.

## INFORMATION, COMMUNICATION & REPORTING

| Principle | Description |
|---|---|
| 18. Leverages Information and Technology | The organization leverages the entity's information and technology systems to support enterprise risk management. |
| 19. Communicates Risk Information | The organization uses communication channels to support enterprise risk management. |
| 20. Reports on Risk, Culture, and Performance | The organization reports on risk, culture, and performance at multiple levels and across the entity. |

Organizations leverage data from multiple technology systems as inputs to support ERM and decisions related to strategic and operational objectives. The requirement for complete, accurate, and relevant information is critical as it serves as the baseline for management's estimates and judgments in various decision-making processes. However, cyber incidents have the potential to impact the reliability of data from compromised systems, especially in instances where the breach is not detected and resolved in a timely manner.

Additionally, in the connected digital environment where decisions must be made in real-time, an important component is not only the reliability of the data, but also the speed at which the data can be reported and consumed. A major threat related to certain cyber incidents is that an incident can impact the availability of an organization's systems and underlying data that is critical for agile risk management and strategic decision making. One example is ransomware that continues to increase in sophistication and has the potential to propagate through and disable an organization's entire network, including connected devices containing critical backups that can no longer be accessed to recover data following an attack (e.g., WannaCry, Ryuk).

> "
>
> Ransomware attackers are hitting both companies and cities with regularity by finding vulnerabilities in their systems, often by sending malicious email attachments, locking up vital data and demanding payments in return for decryption keys.
>
> These attacks happen every day and many are never publicized, cybersecurity professionals say. Local governments can be particularly vulnerable if they lack resources to upgrade equipment and security and protect backup data.
>
> Source: The Wall Street Journal, "Hackers Strike Another Small Florida City, Demanding Hefty Ransom," Jon Kamp and Scott Calv.

Organizations may also benefit from information systems and tools that can be used to facilitate cyber risk management and reporting as many software companies offer governance, risk, and compliance ("GRC") and Integrated Risk Management ("IRM") systems that include standard compliance rulesets for specific technology platforms. In addition, Security Information and Event Management ("SIEM") systems provide valuable tools for event-driven reporting and automation to help resolve alerts real time and categorize alerts based on severity, incident type, relevant devices, number of occurrences, etc., to support the resolution process.

Cyber security monitoring and reporting can also be provided by a third party as a managed service, which can be a valuable investment for organizations with limited IT resources or supporting tools. However, in the event that tasks related to cybersecurity are outsourced, it is essential for the organization to perform the following:

- Maintain regular communication with the service provider for awareness of incidents
- Discuss new and potential threats as the organization's business environment changes and cyber threat landscape continues to evolve
- Provide open communication lines for immediate escalation when a significant incident or breach occurs.

The ability for an organization to communicate both internally and externally on matters relating to cyber risk is imperative as being agile and capable of quickly addressing new and emerging threats to the organization in a timely manner can help prevent or mitigate the impact of significant cyber events. For example, most entities have multiple formally established internal communication channels that are used in tandem with incident response programs. These communication channels are designed to alert employees when real-time events are detected, such as a large-scale phishing attempt impacting an organization's email users. In situations such as this, the entity may choose to alert all corporate email users to make them aware of the situation and reinforce policies on handling and reporting suspicious emails. Some programs also enable organizations to track which employees have received, opened, or deleted these emails. This messaging can be delivered both in an email campaign sent to the entity's internal email address book, and also in the form of an alert published on the entity's internal intranet site. It is equally important for an organization to focus on open communication channels with internal resources and third-party service providers, especially service providers that have access to the organization's data.

The following quote is an excerpt from the Securities and Exchange Commission's Press Release related to the adoption of Interpretive Guidance on Public Company Cybersecurity Disclosures.

"

I believe that providing the Commission's views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors," said SEC Chairman Jay Clayton.

Source: U.S. Securities and Exchange Commission, "SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures."

Organizations need to take a holistic view of not only the purpose of systems in their IT environment, but the type of data that may be stored in each to sufficiently address potential cyber threats. For example, an organization uses a cloud-based ticketing system for tracking system changes and critical incidents. As part of management's ERM program, the risk of a cyber breach is deemed lower as the ticketing system is not considered a critical application because it does not process transactions and is not used to manage customer data. However, a lack of awareness and training may lead to instances where users attach supporting documentation to tickets that contain confidential data, server IP addresses, user credentials, etc., and can be used to exploit various entry points in the organization's network.

Similarly, being able to communicate with external stakeholders on cyber related matters is equally as important. It is imperative to understand communication requirements outlined in various security regulations, both domestically and globally. Failure to make disclosures of incidents with appropriate depth, response, and timeliness may result in significant fines from multiple entities. In today's world, technology allows entities to engage with external stakeholders in a variety of ways ranging from an email message seeking feedback on their most recent customer experience during a transaction, to secure messaging functionality built into an online customer portal reminding them that an upcoming payment is due, to informing them via mail or email of a data breach that may impact their PII. Having a program in place to determine the appropriate method of communication with external stakeholders based upon the nature, sensitivity, and urgency of the communication is a critically important part of achieving the entity's overall ERM program.

Organizations will also need to consider requirements to disclose information related to cyber incidents with other companies, government agencies, and other regulatory bodies. In the United States, guidance provided by the Federal Trade Commission in the article "Data Breach Response: A Guide for Business" describes how most states have enacted legislation requiring notification of security breaches involving personal information. In addition, there may be other laws or regulations that are applicable based on the business, therefore, impacted organizations are responsible for reviewing state and federal laws or regulations for specific reporting and disclosure requirements.[11] Additionally, the Securities and Exchange Commission has released various cyber security regulations and guidance for issuers/public companies, investment advisors, brokers and dealers, and self-regulatory organizations, and established a separate division, known as the Cyber Unit, for cyber-related enforcement actions and penalties related to non-compliance.[12] And, New York Department of Financial Services has a cyber security regulation with which many financial service companies must comply.[13]

For an ERM program to sufficiently identify and enable the entity to appropriately respond to cyber risks, an organization must implement a clearly defined process for relevant and timely reporting at various levels. Organizations may leverage an existing ruleset, such as the AICPA's Cybersecurity Risk Management Reporting Framework, to establish a baseline and facilitate this process. The reporting must be tailored to each specific audience (e.g., information security team, cyber risk management team, executive management, board of directors) as the relevant facts and level of detail required will likely differ between the relevant parties. Minor incidents and more detailed incident data must be reported to the information security team or cyber risk management team and resolved on a regular basis whereas more severe incidents involving a loss of assets or system outages may require escalation to executive management and, in certain instances, the board of directors. Management should have a detailed understanding with the board on the types and severity of instances that will be communicated to them.

Pre-defined procedures can significantly help organizations prepare and respond to cyber incidents. Developing step-by-step instructions and practicing the steps in a simulated environment, similar to a disaster recovery event, can help reduce the amount of response time and organizational impact. Additionally, the definition of key indicators in the ERM program related to cyber risk is equally important as a lack of a breach does not necessarily validate the sufficiency of the cyber risk program and risks continue to evolve along with the deployment of new processes and technology.

> "We encourage companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure.
>
> Source: SEC's Statement and Guidance on Public Company Cybersecurity Disclosures (17 CFR Parts 229 and 249).

Information, Communication, & Reporting are key to sharing indicators which can be used to prevent, detect, or respond to cyber incidents.

## CONCLUSION

Cyber security continues to evolve as bad actors seek to leverage disruption and digitization as launch points for cyber intrusion. Leading organizations will need a structured approach to manage enterprise cyber risk. COSO's ERM Framework provides a foundation upon with a cyber security program can be built, integrating cyber risk management concepts with elements of strategy, business objectives, and performance, which can result in increased business value.

This guidance provided insights into how an organization can leverage the five components and twenty principles of effective risk management to improve its capabilities to identify and manage cyber risks. By using this guidance as a foundation and embracing one or more of the previously mentioned cyber security frameworks (e.g., NIST, ISO, or AICPA), organizations can be better prepared to manage cyber risk in this digital age.

It is imperative for those charged with governance—including the board of directors, members of the audit committee, and business executives—to drive a strong tone at the top, communicate a sense of severity and urgency, and challenge the status quo of their ERM programs and cyber security awareness throughout every level of the organization. Cyber defense and risk management is a shared responsibility of every employee and the extended enterprise. Cyber threats continue to rapidly evolve and increase in complexity each and every day, requiring an organization's leadership, third-party service providers, and employees to not only be prepared for how to respond to a sophisticated attack or breach but also remain one step ahead of new or unknown vulnerabilities. A business-as-usual approach to cyber risk management is no longer capable of achieving these objectives and bound to result in catastrophic damage for stakeholders at every level of the organization.

# APPENDIX

**Cybersecurity Frameworks – Illustrative Examples**

| Sponsoring Organization | Framework | Intended Use | Framework Description |
|---|---|---|---|
| **National Institute of Standards and Technology (NIST)** | NIST Cybersecurity Framework | General Standards | This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.<br>Source: https://www.nist.gov/cyberframework |
| **The Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS)** | N/A - Sector-Specific Guidance based on NIST Cybersecurity Framework | Industry-Specific & Country Specific Standards | The Cybersecurity and Infrastructure Security Agency (CISA) provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, shares that knowledge to enable better risk management, and puts it into practice to protect the Nation's essential resources.<br>CISA relies upon the NIST Cybersecurity Framework but also provides sector-specific guidance for critical infrastructure sectors (e.g., Chemical, Commercial Facilities, Critical Manufacturing, Federal, Healthcare & Public Health, etc.).<br>Source: https://www.us-cert.gov/resources/cybersecurity-framework |
| **International Organization for Standardization (ISO)** | ISO 27001/2 | General Standards | The ISO/IEC JTC 1/SC 27 standard maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management system (ISMS) family of standards.<br>Through the use of the ISMS family of standards, organizations can develop and implement a framework for managing the security of their information assets, including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.<br>Source: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en |
| **American Institute of Certified Public Accountants (AICPA)** | Cybersecurity Risk Management Reporting Framework | General Standards | The AICPA has developed a cybersecurity risk management reporting framework that assists organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs. The framework is a key component of a new System and Organization Controls (SOC) for Cybersecurity engagement, through which a CPA reports on an organizations' enterprise-wide cybersecurity risk management program. This information can help senior management, boards of directors, analysts, investors and business partners gain a better understanding of organizations' efforts.<br>Source: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html |
| **Payment Card Industry (PCI) Security Standards Council** | Payment Card Industry Data Security Standard (PCI DSS) | Industry-Specific Standards | The PCI Security Standards Council touches the lives of hundreds of millions of people worldwide. A global organization, it maintains, evolves and promotes Payment Card Industry standards for the safety of cardholder data across the globe.<br>Maintaining payment security is required for all entities that store, process or transmit cardholder data. Guidance for maintaining payment security is provided in PCI security standards. These set the technical and operational requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.<br>Note: The PCI Security Standards Council provides illustrative mapping of the PCI DSS framework to the NIST Cybersecurity Framework.<br>Source: https://www.pcisecuritystandards.org/pci_security/ |

# APPENDIX (cont.)

| Cybersecurity Frameworks – Illustrative Examples | | | |
|---|---|---|---|
| **Sponsoring Organization** | **Framework** | **Intended Use** | **Framework Description** |
| **HITRUST Alliance** | HITRUST CSF | General Standards | HITRUST has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from the public and private sectors, HITRUST develops, maintains and provides broad access to its widely-adopted common risk and compliance management frameworks, related assessment and assurance methodologies.<br>Source: https://hitrustalliance.net/about-us/ |
| **Center for Internet Security** (formerly sponsored by SANS) | CIS Controls Version 7.1 | General Standards | Organizations around the world rely on the CIS Controls security best practices to improve their cyber defenses. CIS Controls Version 7.1 introduces new guidance to prioritize Controls utilization, known as CIS Implementation Groups (IGs). The IGs are a simple and accessible way to help organizations classify themselves and focus their security resources and expertise while leveraging the value of the CIS Controls.<br>Source: https://www.cisecurity.org/controls/ |
| **ISACA** | COBIT 2019 – Governance & Management Objectives | General Standards | COBIT is a framework for the governance and management of information and technology.<br>The COBIT framework makes a clear distinction between governance and management. These two disciplines encompass different activities, require different organizational structures, and serve different purposes.<br>The COBIT® 2019 Framework: Governance and Management Objectives comprehensively describes the 40 core governance and management objectives, the processes contained therein, and other related components. This guide also references other standards and frameworks.<br>Source: http://www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Governance-and-Management-Objectives.aspx |
| **Cloud Security Alliance (CSA)** | Cloud Security Alliance Cloud Controls Matrix (CCM) | Technical-Specific Standards | The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the CSA guidance in 13 domains. The foundations of the CSA Controls Matrix rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP and will augment or provide internal control direction for service organization control reports attestations provided by cloud providers.<br>Source: https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/ |

# REFERENCES


1. Committee of Sponsoring Organizations of the Treadway Commission, COSO Enterprise Risk Management Framework, 2017.
2. Deloitte's 2019 Future of Cyber Survey, in conjunction with Wakefield Research, polled 500 C-level executives who oversee cybersecurity at companies with at least $500 million in annual revenue including 100 CISOs, 100 CSOs, 100 CTOs, 100 CIOs, and 100 CROs between January 9, 2019, and January 25, 2019, using an online survey.
3. Khalid Kark, Caroline Brown, Jason Lewris, Bridging the boardroom's technology gap, Deloitte University Press, June 29, 2017.
4. National Institute of Standards and Technology (NIST), "Framework for improving critical infrastructure cybersecurity," April 16, 2018.
5. Marc Kaplan, et al., "Shape Culture, Drive Strategy," Global Human Capital Trends 2016, Deloitte University Press, 2016.
6. Deloitte Wall Street Journal article. deloitte.wsj.com/cio/2019/07/11/cyber-incidents-and-breaches-the-data-dilemma/.
7. National Institute of Standards and Technology, Cybersecurity Framework. nist.gov/cyberframework.
8. International Organization for Standardization. iso.org/.
9. American Institute of Certified Public Accountants, System and Organization Controls for Cybersecurity, USA, 2017. aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html.
10. American Institute of Certified Public Accountants, System and Organization Controls for Cybersecurity, USA, 2017. aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html.
11. Federal Trade Commission, "Data Breach Response: A Guide for Business", April 2019 ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.
12. Securities and Exchange Commission, "Spotlight on Cybersecurity, the SEC and You", retrieved September 2019, sec.gov/spotlight/cybersecurity.
13. New York State Department of Financial Services, "Cybersecurity Requirements for Financial Services Companies", effective March 2017 dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

## ABOUT THE AUTHORS

### Mary E. Galligan, Managing Director, Deloitte & Touche LLP

Mary Galligan is a managing director in Deloitte's Cyber practice. Mary advises senior executives on the crisis management challenges they face, in particular cyber risks. She helps clients develop and execute security programs to prevent and reduce 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 take shape. Mary has provided cyber awareness briefings to more than 70 boards of directors at privately held, as well as Fortune 500, companies. She has presented at numerous NACD events as well as at Stanford's Directors College. Due to her leadership in cyber risk and crisis management Mary is frequently asked by both print and TV news outlets to comment on developing cyber events.

Mary joined Deloitte after retiring in 2013 from a distinguished career with the Federal Bureau of Investigation (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 Doctor of Law from Marian University, Fond du Lac, Wisconsin. She is a FBI-certified Crisis Negotiator and Crisis Manager.

### Sandy Herrygers, Partner, Deloitte & Touche LLP

Sandy leads Deloitte's Global Assurance market offering and US Information Technology Specialist Group. She has spent her career focused on internal controls and information security in the Consumer and Industrial Products and Financial Services industries. She has been in the Risk & Financial Advisory practice since 1998 and has practiced in the Chicago and Detroit offices.

Sandy leads our internal control audit services to several large, global clients of Deloitte. In that capacity, she leads entity-level, business cycle, and information technology testing areas. This role includes skills such as leading large, cross-border Deloitte teams and dealing with fully outsourced, complex, and diverse information technology environments and rapidly changing and challenging business and internal control environments.

From a leadership perspective, Sandy oversees the quality of IT audit services, including functioning as a consultation resource for IT and internal control related matters on the largest and most complex integrated audits. Further, she leads development of audit approach methodology, tools, practice aids and learning for IT specialists.

Sandy represents Deloitte on several outside initiatives related to information security and internal control including the Center for Audit Quality Cyber Working Group and the AICPA ASEC Cyber Security Working Group.

### Kelly Rau, Managing Director, Deloitte & Touche LLP

Kelly Rau is a managing director within Deloitte's Risk & Financial Advisory practice, specializing in Assurance & Internal Audit offerings. Kelly joined Deloitte in 2002 and has extensive experience in assisting companies with a variety of internal control and information technology matters. Through engagement 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 has been a member of 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 our 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

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 our legal structure.
Certain services may not be available to attest clients under the rules and regulations of public accounting.


COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org


# MANAGING CYBER RISK IN A DIGITAL AGE

COSO

Committee of Sponsoring Organizations of the Treadway Commission

coso.org