www.pwc.com

Directors and IT

A user-friendly board guide for effective information technology oversight

Abridged version
2016

pwc

About this publication

This abridged version of *Directors and IT*, a user-friendly guide for effective information technology (IT) oversight, highlights a six-step process that directors can follow to better fulfill their IT oversight responsibility. The unabridged guide (the Guide) includes a number of other supplemental tools for directors, including an IT oversight checklist to help execute the process; discussion of the background, rewards, risks, and board considerations for various IT subjects (e.g., data security, social media, and cloud services); and questions directors can ask about the IT subjects most relevant to their company.

This abridged version and the Guide were created as part of our commitment to providing directors with leading practice guidance for being effective in the boardroom. We have updated this report to reflect the evolution of technology risks and to provide the most up-to-date information and suggestions as you navigate your related oversight responsibilities.

About PwC's Center for Board Governance

PwC's Center for Board Governance helps directors effectively meet the challenges of their critical roles. We do this by sharing leading governance practices, publishing thought leadership materials, and offering forums on current issues. We also meet with boards of directors, audit committees, and executives to share our insights into significant governance challenges and developments.

Find more information at ***www.pwc.com/us/CenterforBoardGovernance***

Introduction: The "IT confidence gap"

Overseeing a company's information technology activities is a significant challenge for directors. The pace of change in this area is rapid, the subject matter is complicated, and the highly technical language used to describe emerging technologies and evolving risks makes this a challenging area. And many companies are relying more and more on technology to get ahead, often prompting substantial changes in how they operate. All of these factors can make the board's IT oversight responsibility appear harder than it is.

Our research, which included surveying approximately 800 public company directors during 2012-2015, indicates many board members are uncomfortable with overseeing their company's IT. Although many directors want to better comprehend the risks and opportunities related to IT, they sometimes don't have an adequate understanding of the subject to be truly effective in their oversight roles. In addition, boards often lack a well-defined process that satisfies their needs in this area. On the whole, this confluence of factors creates an "IT confidence gap" for many board members. Consider the following:

- *Many directors grew up in a predigital age:* Board members have an average age of around 63,[1] and most of their professional lives were spent in a predigital era. New technologies such as social media and cloud computing have only recently entered the scene.
- *Very few directors have IT backgrounds:* Less than 1% of Fortune 500 directors have been or are currently Chief Information Officers (CIOs).[2] This limited experience working directly with IT can contribute to a lack of confidence in a director's ability to oversee the strategic use of IT and related risks.
- *Board time is at a premium:* Almost 65% of directors would like their boards to devote more time in the coming year to IT risks and 46% to IT strategy.[3] This is despite the fact that many directors are currently dedicating a considerable chunk of their board hours to the subject. Fifty-five percent of current board members spend more than 5% of their total board time discussing and considering IT risks and opportunities; almost one in five spend 11% or more.[3]

"Regulators have given indications that they expect boards to improve oversight and reporting on risks, with IT risks being a special focus. This Guide will help boards prepare for the responsibility."

—Director

- *Directors want more information:* Directors' concerns about IT suggest they do not underestimate its importance to the enterprise. In fact, the majority are hungry for more information about the company's approach to managing the fundamental aspects of IT: Less than a third of directors "very much" believe their company's approach to managing IT risk and strategy provides the board with adequate information to be effective.[3]

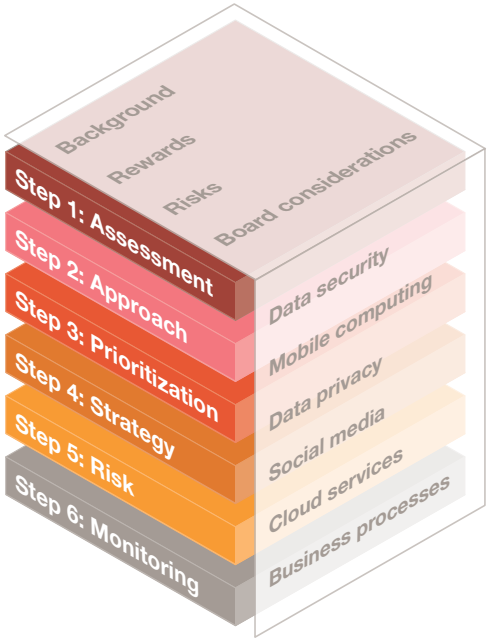
What can the board do to bridge the "IT confidence gap?" Structured frameworks for IT professionals and management already exist; however, they are not designed with the board's oversight role in mind. To fill this void, PwC developed the Guide, which introduces our IT Oversight Framework, to help boards figure out how to best oversee IT at their companies.

For many boards, cybersecurity has moved to the forefront of director concerns, and they are myopically focused on this issue. However, we suggest boards take a step back and look at IT more broadly and in a holistic manner.

The IT Oversight Framework is a six-step process that:

- embraces IT oversight in a cohesive, comprehensive and holistic manner;
- provides a structured approach for boards to help with their oversight responsibilities;
- offers flexibility for customization based on the company's specific circumstances;
- includes leading oversight practices to facilitate discussions with the CIO, company management, or outside consultants; and
- may help identify IT issues that may not currently be on management's or the board's radar.

The IT Oversight Framework



Step 1—Assessment:

Determine how critical IT is to the company and the current state of its infrastructure

It is essential for directors to understand how important IT is to the company's success before the board can make decisions about its proper IT oversight approach. Directors should begin by considering the role IT plays in the company's industry and various attributes of the company, such as:

- the existing business model and expected changes;
- the current state of IT infrastructure ("IT health"); and
- the budgeted IT spend.

These types of baseline considerations are generally relevant to every type of company and arm directors with the necessary knowledge to agree on the best approach to IT oversight.

The role IT plays in the company's industry

For some companies, IT is an essential element of their business model and is often an integral part of the industry they're in. For example, a large financial institution could not survive without the systems that process millions of transactions each day, such as deposits, cash transfers, and credit card charges and payments. For companies in other industries, IT might be less essential, used primarily for back-office support in areas such as bookkeeping and payroll. At these companies, the priority might be maintaining existing IT systems, with considerably less focus on adopting emerging technologies such as social media or cloud services.

Existing business model and expected changes

There are numerous factors directors can consider when evaluating the best approach to IT oversight, including:

- *Current business issues*—Major changes in the economy or in the company's markets that significantly impact the company's bottom line; variables such as changing customer markets, the exploitation of which depends on the ability to leverage new technology platforms like social media and mobile computing.
- *"Crown jewels"*—An understanding of the company's most valuable and sensitive digital data and mission-critical systems and how they are maintained can be useful. Crown jewels are fundamental to the brand, business growth, and competitive advantage. Examples include trade secrets, market-based strategies, product designs, new market plans, or other critical business processes. Relevant baseline information should emphasize that protections over these digital assets are critical.
- *Sensitive customer information*—The custody of credit card numbers, health records, and other personal customer data.
- *Mergers and acquisitions*—Planned acquisitions that will require the company to merge disparate IT systems, the consolidation of which could impact the company's ability to produce reliable and timely financial reporting and maintain its operating efficiency.
- *Major IT system implementations*—The installation of new enterprise resource planning (ERP) systems or adoption of the cloud (or another emerging technology).
- *Level of IT outsourcing*—The level of IT outsourcing relative to the overall IT spend.
- *Regulatory requirements*—IT systems built to comply with new rules or regulations.

IT health check

The board should understand management's assessment of the current state of the company's hardware and software infrastructure, including:

- whether the company has put off upgrading its systems, resulting in a deferred IT maintenance backlog;
- whether efforts are under way to improve IT productivity;
- the recent track record of systems stability; and
- the level of IT systems integration from prior acquisitions or mergers.

Other aspects of the company's IT health that should also be evaluated include:

- *Coverage by a cyberinsurance policy*—Directors should understand whether the company has cyberinsurance coverage and the rationale behind the decision. If coverage exists, knowledge about what the policy will cover (and, more importantly, what it doesn't cover), levels of coverage, policy limits, and other relevant matters is important.
- *Evaluation of the tone at the top*—Directors should evaluate the extent and rigor of senior management's communications focusing on the importance of cybersecurity at the company. More than any other threat actors, current and former employees are the most cited culprits of security incidents.[4]
- *Current and desired state of cybersecurity program*—A risk framework is used by a company to help think through, organize, and evaluate its cybersecurity risk program. There is not a prescribed framework or a one-size-fits-all solution addressing an effective structure. Directors should have baseline information about the company's current cybersecurity program relative to an established framework. This should include how it compares to that framework, an assessment of identified gaps, and the proposed action plan and timeline to improve it.

The IT budget

Many boards are already engaged in understanding the company's IT budget: 67% are either "very" or "moderately" engaged in doing so (an increase of 10 percentage points from 2012), but 32% believe that their involvement is "not sufficient" or they are not engaged at all.[3] However, the majority of boards that are not reviewing the budget consider IT to provide merely back-office infrastructure to their company.

One factor to consider when reviewing the IT budget is how the company has allocated spend for IT innovation versus basic IT maintenance. Directors should understand whether the company is spending enough on IT for the future, or if it is doing just enough to "keep the lights on." Another consideration is the ratio of IT spend to company revenue relative to others in the industry. If the company's spend compares unfavorably to others, increased IT oversight may be necessary.

Using baseline information to decide on the best approach

Directors should consider all of the variables noted above and use their knowledge of the company to assess the importance of IT to the company to develop a tailored approach to IT oversight.

Step 2—Approach:

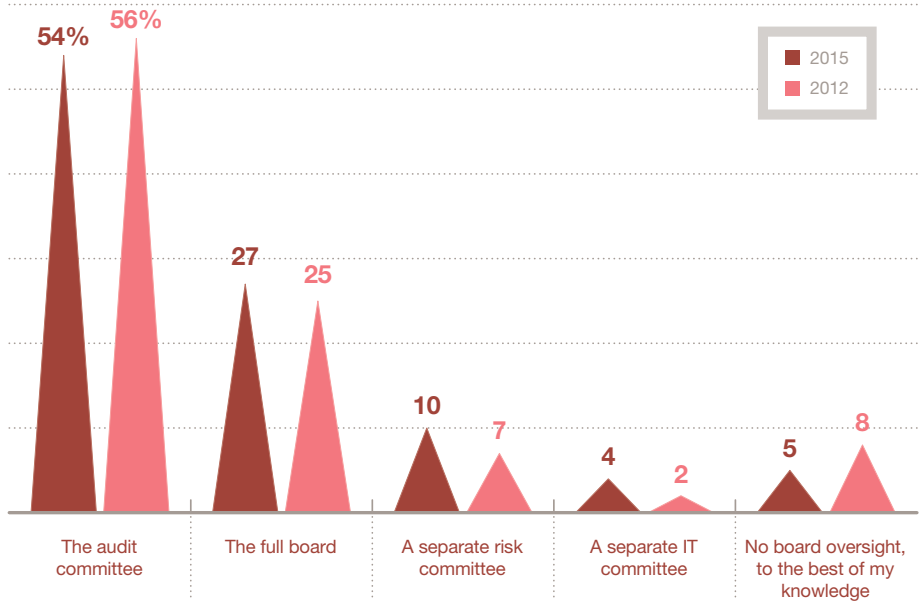
Agree on the board's IT oversight approach

When deciding on the best board approach to IT oversight, directors should evaluate whether the board or a specific committee of the board will "own" IT oversight and whether the appropriate resources are available. This decision includes considering whether to add IT expertise to the board or engage outside consultants.

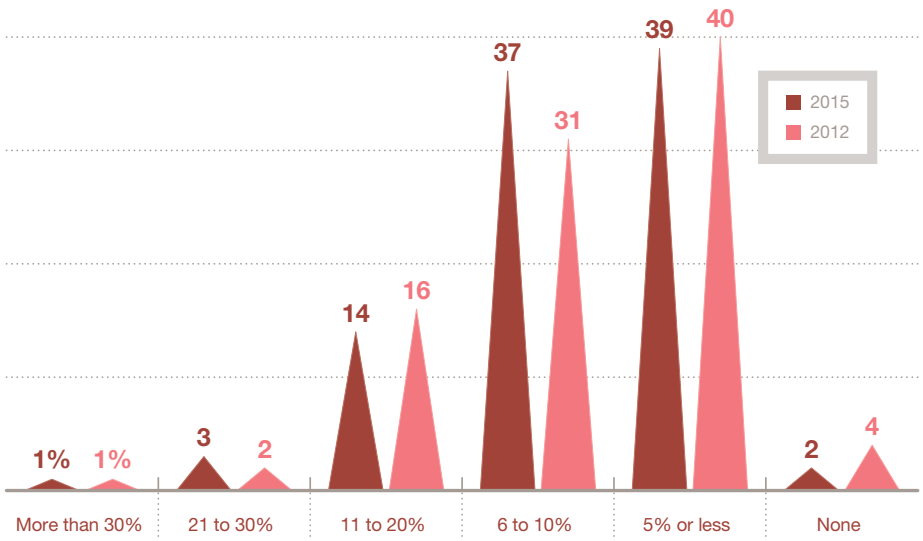
Who should provide IT oversight

In our research, 54% of directors say the audit committee is responsible for IT oversight.[3] This committee often oversees the company's risk management process, and IT is usually discussed from a risk perspective. Twenty-seven percent of directors assign IT oversight to the full board, while only 10% of directors use a separate board-level

Who on the board currently has primary responsibility for the oversight of IT risks?[3]



On average, what percentage of last year's total annual board/ committee hours were spent discussing oversight of IT risks and opportunities?*[3]



* Excludes "don't know" responses

risk committee.[3] Even fewer boards have established a separate board IT committee—most of whom are those that believe IT is "critical" or "very important" to their company's success. Regardless of whether the full board or a committee is given the oversight task, the board should consider the backgrounds and experience of existing directors to decide if they have the skills necessary to oversee IT. If not, the question is whether the board should add IT expertise, particularly for companies that determine IT to be of greater importance to their business. If so, there are a couple of options:

- *Bring IT experience onto the board:* Boards can dedicate one or more seats to someone with an IT background, such as a current or former CIO. For companies that consider IT critical, having such a resource may be particularly important. But this approach is not favored by most board members, as only 37% of directors believe it is very important to have directors with IT strategy expertise on today's boards and 33% say this about cyber risk expertise.[3]
- *Use outside expertise:* An increasing number of boards are using external consultants to advise them on IT: 45% of boards engaged outside consultants to provide guidance on IT during the last year (80% of the consultants were hired for specific projects), up from 27% in 2012.[3]

How often should directors discuss IT?

Once the board determines who will provide IT oversight, directors should decide how often to meet and discuss IT issues, as well as when to communicate with the CIO. The percentage of total board hours dedicated to IT oversight continues to rise with 55% of directors spending over 5% of their hours on it (versus 50% in 2012).[3]

Our study indicates that today's boards are increasingly communicating with the company's CIO; 25% do so at every formal board meeting (versus 18% in 2012) and 34% do so at least twice a year.[3] Only 10% are not communicating at all.[3]

Step 3—Prioritization:

Identify the IT subjects most relevant to the company

Now that the approach has been decided, the group charged with oversight responsibility needs to prioritize which IT areas are most relevant to the company. We have summarized the most common contemporary IT topics below to facilitate this prioritization.

We have also included a few board considerations for each topic; an expanded list appears in the unabridged version of the Guide. Of course, each of these topics may not be relevant to every company.

IT subject	Board considerations
Data security—Cybersecurity is a major challenge for many companies. Successful cyberattacks can cause significant damage to a company's business and reputation.	Understand the company's perceived level of security risk, comprehensive security strategy, the controls designed to mitigate the risk, and the status of controls relative to an established framework. Understand who is ultimately responsible for security and whether tone at the top emphasizes its importance. Determine how management tests resistance to attacks. Ask management about the company's IT security resources and whether the security spend level is appropriate.
Mobile computing—Mobile is ubiquitous and presents huge market opportunities. Devices are more affordable and provide significantly greater access to company data by employees and others.	Understand the role mobile is playing in the changing global economy and evaluate the appropriateness of a mobile strategy. Understand the company's policy for allowing employee use of personal mobile devices to access corporate data. Discuss how the company's mobile policy is communicated to employees and how they are trained in its implementation.

IT subject	Board considerations
Data privacy—Many companies keep sensitive customer data. The efficacy of the company's internal and external privacy policies may be critical to avoiding big problems.	Understand how the company protects sensitive data from the risk of theft. Understand the company's internal and external data privacy policies. Ask management about privacy policies related to any data exchanges with third parties. Set the expectation that management will keep the board up to date on privacy laws and regulatory developments.
Social media—Social media is an essential tool for many companies and for their customers and employees. Directors should be aware of both rewards and risks involving how the company and its employees use social media.	Take interest in how the company and its competitors use social media to engage customers, develop markets, and recruit talent. Understand whether the company knows what is being said about it on social media platforms. Discuss how employees use social media at work and what safeguards exist to protect the brand.
Cloud services and software rentals—Using the Internet to access hosted computing power that can often lead to lower cost, faster implementation, more flexibility, and greater accessibility. But it is not without risk. Many companies are using, or plan to use, cloud strategies.	Ask management about their pursuit of cloud strategies and cost-benefit considerations. Discuss security and privacy risks associated with using the cloud, including backup and recovery. Inquire about existing regulations and compliance risks of cloud computing.
Streamlining business processes using Big Data and other digital means—Many companies are leveraging IT to enhance their performance. Advantages can include operating and workforce efficiencies, lower costs, and integration of supply chains and distribution channels. Companies are also finding ways to analyze large amounts of information and use it to their advantage.	Ask how executives are leveraging IT to enhance communications. Understand the use of Big Data to give the company a competitive edge.

After considering various IT subjects that are part of technology today and asking the right questions, the board members responsible for IT oversight should decide which topics deserve the most attention. They should prioritize those topics for specific focus to efficiently use their time.

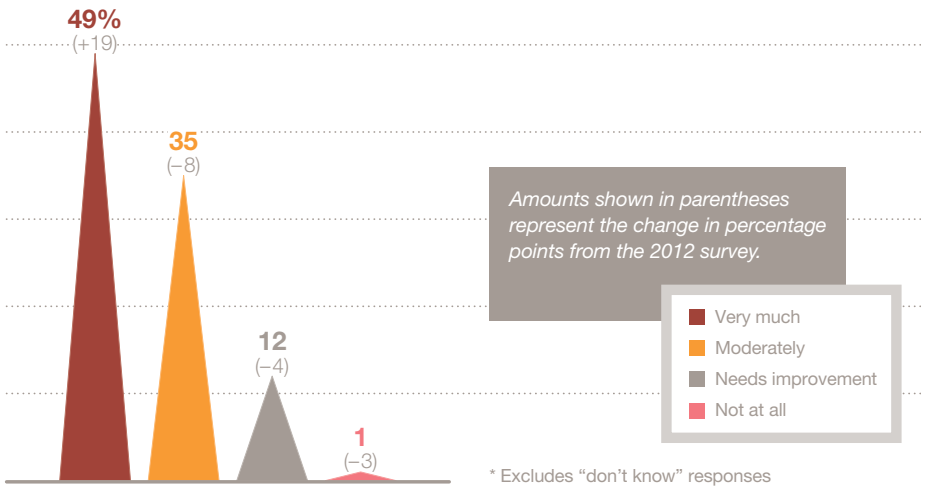
Step 4—Strategy:

"Bake" IT initiatives into strategy oversight

Directors should ensure IT considerations are integrated into the board's ongoing review of the company's strategy. The more critical IT is to the company, the deeper the board should probe the company's plans for using technology to facilitate execution of an effective strategy.

Directors are now much more comfortable with their company's approach to managing IT strategy and risk than they were three years ago with almost half of them "very much" believing it contributes to and is aligned with setting overall strategy (an improvement of 19 percentage points).[3]

Do you believe the company's approach to managing IT strategy and risk contributes and is aligned with setting overall strategy?*[3]



* Excludes "don't know" responses

"It is important for the board to understand how IT innovation can bring opportunity."
—Thought leader

As IT becomes increasingly embedded in overall company strategy, it is more important to understand how current and emerging technologies work across the various functions within the company. Boards should discuss with management how people throughout the company are working together to understand new IT developments. This can include employees in business development, marketing, sales, public relations, and human resources. Directors should also inquire whether management has adopted an enterprise-wide approach that considers the holistic needs of the entire company when making strategic IT decisions. This can help prevent a silo approach to IT strategy, which could end up being more costly and less effective.

It is important for directors to understand the company's key technology priorities—for the short- and long-terms. Management's approach to making these determinations can provide perspective to boards. Examples of tools commonly used are:

- return on investment analyses;
- scenario modeling;
- analyses of strengths, weaknesses, opportunities, and threats associated with specific technologies;
- competitive analyses; and
- research and analyses of the timing of emerging technologies yet to hit the market.

Thinking about IT as a tool for innovation can help directors close the "IT confidence gap." Effective use of IT usually occurs if it is planned in advance with a concerted effort and focus and a well-executed plan. Considering IT as part of the company's overall strategy also better allows the board to recognize the potential benefits of newer technologies, such as mobile computing and social media, and the impact they could have on the company's bottom line.

Step 5—Risk:

"Bake" IT into risk management oversight

IT risks need to be included in the company's overall risk management process and its risk oversight process, even as new technologies change the profile of risk over time. Some of the more enduring IT risks include the risk of:

- failure to execute on strategic IT goals;
- an inability to protect personal and sensitive data;
- breakdowns in IT systems that limit the company's operations;
- missed opportunities to take advantage of emerging technologies;
- failure to keep up with competitors' use of IT; and
- noncompliance with IT laws and regulations.

Effective risk management entails identifying the most significant IT risks, the probability of a negative event occurring, and its potential impact. Boards should make sure that key individuals outside IT have input into the IT risk management process. These may include the Chief Risk Officer, Chief Privacy Officer, Chief Information Security Officer, business unit leaders, internal and external auditors, or even outside consultants.

It is helpful for boards to communicate to management about the specific information they would like to receive to effectively oversee the IT risk management process.

Companies should consider how the top IT risks can best be mitigated through effective internal controls. Risk reduction procedures are effective only if they are woven into the fabric of the entire organization. Directors should ask management whether company policies and training programs are updated to reflect the changing IT risk environment. Often, employee communications may need to be enhanced, including how to report IT policy violations or issues.

Things can go wrong far too easily (and do go wrong far too frequently) for directors not to discuss crisis management as part of their risk management oversight. One aspect of crisis management planning is how the company communicates in a crisis, including how it intends to use technology. Boards should ask whether it makes sense for the company's crisis communications plan to embrace social media as a way of reacting quickly when a negative event arises. Doing so may ensure the company's version of the story gets heard. Our research finds 54% of directors are "not sufficiently" or not at all engaged in understanding the company's social media crisis communications response plan.[5]

"Our board is spending a lot more time discussing IT risks, including those related to new technologies."

—Director

Step 6—Monitoring and cybermetric reporting:

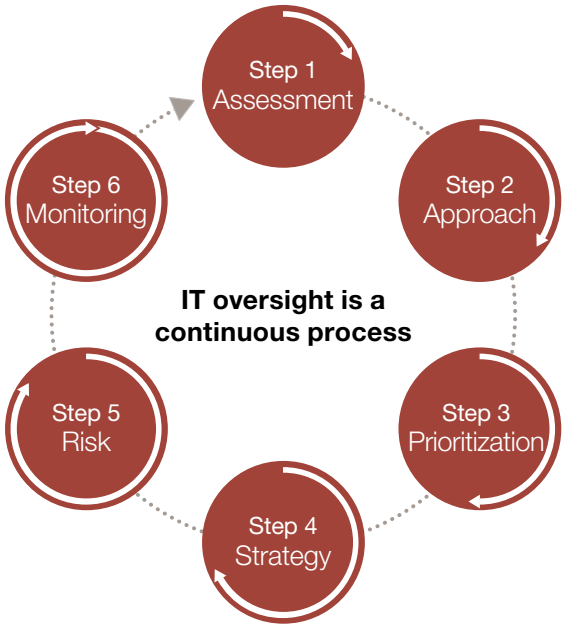
Adopt a continuous process and measure results

Board oversight should be the safety net for ensuring that a comprehensive IT program supported by the chief executive officer and senior management is followed by the company. However, the rapid pace of IT change can cause previous conclusions about the board's approach to IT oversight to become stale quickly. Directors will want to know whether there are any changes to the company's IT plans or new strategic initiatives and their underlying risks.

Decisions about the importance of IT to the company (Step 1), the board's approach (Step 2), identification and prioritization of the most relevant IT issues (Step 3), and the integration of IT into strategy and risk management (Steps 4 and 5), should be revisited at least annually.

- *Consider regular IT updates to address whether planned IT activities are being implemented effectively and in a timely manner:* Directors should define how often they will receive these updates from management. The frequency of board discussions with the CIO and the amount of hours the board is spending on IT oversight may also need to be readdressed based on changing facts and circumstances.
- *Determine which key performance indicators and cybermetrics they expect to receive from management on an ongoing basis:* Reporting should address most, if not all, baseline information referenced in Step 1 relative to understanding the existing business model and expected changes, the current state of the company's IT infrastructure, and the budgeted IT spend. In addition to baseline information, directors need to define the right cybermetric data that is most important to succeed in effective oversight at their company. The cybermetrics should be reported to the board on an ongoing basis and can include specific information about such topics as data security, privacy, social media, Big Data, cloud computing, and mobile computing. It may be helpful to create a director's dashboard to capture these metrics.

The key is to initially define a process that works best for your particular board and then put the process in place. Ongoing monitoring of the effectiveness of the company's IT activities should be supplemented by a continuous evaluation of the board's oversight process. Not only does the business change and technology evolve, but the composition of the board and its level of IT expertise fluctuates. Periodic "fresh looks" at the framework will provide directors with confidence in their IT oversight.



The bottom line

As technologies continue to evolve, directors will likely face more IT oversight responsibilities. Therefore, implementing a defined process for board oversight can provide distinct advantages over an ad hoc or poorly defined approach. Following an agreed-upon methodology can promote a thorough, disciplined, and rigorous board oversight process. We believe that use of the IT Oversight Framework enables directors to bridge the "IT confidence gap" and rest more comfortably knowing a robust oversight process is in place.

Directors can obtain more detailed information about effective IT oversight by reading the complete Guide.

Endnotes

1 Spencer Stuart US Board Index 2015.
2 Diamond Management & Technology Consultants, "How does a CIO become a Fortune 500 board member?" 2009.
3 PwC, *Annual Corporate Directors Survey*, 2015.
4 PwC, *Global State of Information Security Survey*, 2015.
5 PwC, *Annual Corporate Directors Survey*, 2013.

pwc.com/us/CenterForBoardGovernance

To have a deeper conversation about how this subject may affect your business, please contact:

Paula Loop
Leader, Center for Board Governance
and Investor Resource Institute
PwC
646 471 1881
paula.loop@pwc.com

Don Keller
Partner, Center for Board Governance
PwC
512 695 4468
don.keller@pwc.com

Barbara Berlin
Director, Center for Board Governance
PwC
973 236 5349
barbara.berlin@pwc.com