www.pwc.com/ca

Board of Governors of Exhibition Place

Audit plan for the year ended
December 31, 2015

January 11, 2016

January 11, 2016

Members of the Finance and Audit Committee of the
Board of Governors of Exhibition Place

Dear Members of the Finance and Audit Committee:

We're pleased to present an overview of our audit plan for the 2015 audit of the financial statements of the Board of Governors of Exhibition Place (the Board) prepared in accordance with Public Sector Accounting Standards (PSAS).

This overview includes our view on audit risks, the nature, extent and timing of our audit work, as well as our proposed fees and the terms of our engagement.

We value your feedback and welcome any suggestions and observations you may have.

Yours very truly,

PricewaterhouseCoopers LLP

Terri McKinnon
Partner
Risk Assurance Services

c.c.: Dianne Young, Chief Executive Officer
Hardat Persaud, Chief Financial Officer

PricewaterhouseCoopers LLP
PwC Tower, 18 York Street, Suite 2600, Toronto, Ontario, Canada M5J 0B2
T: +1 416 863 1133, F: +1 416 365 8215, www.pwc.com/ca

Communications to the Audit Committee

Key matters for discussion	*Comments*
Client service team	• Terri McKinnon is your engagement leader and Marisa Troina is your engagement senior manager.
Service deliverables	• We will audit the Board's financial statements as of December 31, 2015 and for the year then ended prepared in accordance with PSAS. • Our engagement letter, which has been signed by the City of Toronto (the City), sets out the terms and conditions for our engagement as the independent auditor of the Board for the above-mentioned year. • In addition, our engagement letter outlines our responsibilities as the auditor and the responsibilities of management.
Audit timeline	• We worked with management to develop this project timeline: o Interim visit: November 1 - 6, 2015 o Year-end visit: March 7 - 18, 2016 o Clearance meeting with management: March 18, 2016 o Year-end Finance and Audit Committee meeting: May 13, 2016 o Delivery/filing of financial statements: TBD
Audit approach	• Our audit approach is a mixture of tests of internal controls and substantive testing. • Significant areas of audit focus are areas that we think need special audit consideration. We identified several areas of audit focus which are described in the section below. Please let us know if you agree that these are the areas of focus from your point of view and if you have any other areas of concern.
Areas to discuss	**Management's response and our audit approach**
Revenue recognition The Board has several significant revenue streams including (but not limited to): • Building rentals and concessions; • Services; and • Parking.	We will obtain an understanding of management's processes surrounding revenue recognition and test controls surrounding the reconciliation and signoff of parking revenues by attendants. We will also perform test of details on significant revenue streams.

Key matters for discussion	*Comments*
Completeness and accuracy of transactions recorded with the City The Board engages in many transactions with the City of Toronto and its various Agencies, Boards, and Commissions (the City).	We will obtain a confirmation of balances from the City held at year-end ensure they reconcile to the records of the Board.
Employee future benefits payable The Board sponsors a defined benefit pension plan to its employees, for which the City fund this obligation. The City has engaged external experts to assist with the valuation of post -retirement and post-employment benefits.	We will obtain the actuarial report and assess the competency and objectivity of experts engaged by the City. We will also incorporate an internal pension expert into our engagement team to assess the appropriateness of accounting estimates applied in the actuarial valuation.
Management override of controls Accounting regulatory authorities require that the risk of material misstatement due to management override of controls be considered a significant risk on every audit engagement. This represents the risk that internal controls of the Board may be circumvented to achieve desired financial results or gain inappropriate access to financial resources.	In order to address this risk, we will perform the following: • Assess the control environment and segregation of duties within the Board; • Review significant and non-standard manual journal entries made during the year; • Review assumptions made by management in making significant estimates; and • Incorporate unpredictable procedures in our audit.
Materiality	• Misstatements are considered to be material if they could reasonably be expected to influence the economic decisions of users of the financial statements. • We have set a preliminary materiality of $1,300,000 based on 3% of projected revenue for the year. • We'll report unadjusted and adjusted items over $130,000 to the Finance and Audit Committee on completion of the audit.

Key matters for discussion	*Comments*
Fraud risk	• We discuss fraud risk annually with the Finance and Audit Committee. • Through our planning process (and prior years' audits), we developed an understanding of your oversight processes including: o Whistle-blower hotline review o Finance and Audit Committee and our attendance at one of those meetings o Presentations by management, including business performance reviews o Review of related party transactions o Consideration of tone at the top • Are there any new processes or changes to the items above that we should be aware of? • We are not aware of any fraud. Are you aware of instances of any actual, suspected or alleged fraud affecting the organization?
2015 audit fees	• The audit fee for 2015 is $25,000, which is based on the RFP covering the five year contract period for the years ended December 31, 2015 through to 2019. • Other audit related fees for the current year included the following: o Ricoh Coliseum-audit of schedule of fixed operating costs for additional rents payable (period ended June 30) for which $8,060 has been billed and paid. o Audit and advisory services relating to the processes and controls surrounding the Board's parking operations. Fees for these services have been quoted as $19,500 for which no amounts have been billed yet. We will commence this work in the coming weeks. • Appendix A contains a copy of our client services guideline.

Appendix A: Client Services Guideline

	Our commitment to you and expectations of the Board	Additional audit services
Audit readiness and monitoring of audit progress	• We will provide a detailed listing of audit information requests and agree with management upfront the required dates to provide the requested information. • We will agree with you the start dates of our interim and year-end audit fieldwork. A completed trial balance that includes all management year-end closing entries will be provided at a date agreed to upfront with management. • We will hold periodic meetings with management (dates and times to be agreed upfront) to discuss the status of the audit. As part of these meetings, we will provide a detailed list of outstanding items and will highlight any items that require more urgent attention and follow up.	• Delays in receiving requested information that results in idle staff time or staffing changes or any changes to the trial balance subsequent to the agreed upon date that results in additional audit testing will be billed separately. • Time incurred to review and/or test multiple versions of client prepared schedules will be billed separately.
Significant accounting and reporting matters	• We will hold meetings with key staff at the Board as part of the audit planning process to understand significant developments and changes for the current year and share with you our views on the accounting and audit implications. • For significant new developments that have an accounting, reporting and/or auditing impact, management will prepare a position paper, in a format as outlined in our summary of audit information requests, summarizing the issue, the technical analysis/research supporting management's position and the impact to the Board.	• Time incurred to review management's position paper and resolve significant accounting matters will be billed separately. • In addition, time incurred to quantify and perform additional audit procedures, as necessary, to validate adjustments will be billed separately.
Financial statement review	• Year-end financial statements and note disclosures will be prepared and reviewed by management and provided to us for our review in accordance with the timelines as outlined in our audit information request listing. • We will review two versions of the financial statements. We will provide our comments, including any suggestions for change to management, on the first version and will review a second version of the financial statements for any changes made as a result of our initial review.	• Significant revisions to the financial statements (i.e. re-writing of note disclosures or pervasive mathematical errors and/or internal inconsistencies) and reviewing multiple versions of the financial statements (i.e. more than two versions) will be billed separately.
Finance and Audit Committee/ Board meetings	• We will attend one meeting at year-end to present our draft year-end audit report (summarizing our key audit findings) to management and discuss any comments or revisions suggested by management.	• Additional meetings with the Finance and Audit Committee/Board and additional drafting sessions or clearance meetings with management will be billed separately.

Appendix B: Cybermetrics – What Directors need to know

Audit Committee Excellence Series

Achieving excellence: Cybermetrics —What directors need to know

September 2015

PwC's Audit Committee Excellence Series (ACES) provides practical and actionable insights, perspectives, and ideas to help audit committees maximize their performance. This edition addresses the cybermetrics that boards need for effective IT oversight.

pwc

This ACES module addresses key elements of reporting effective cybermetric information to directors:

1. Why the right cybermetrics are critical to audit committees
2. Who, what, and how is important
3. Figuring out the cybermetrics that matter most
4. It's a changing world and continuous process

1. Why the right cybermetrics are critical to audit committees

Overseeing a company's IT initiatives, particularly the adequacy of cybersecurity, can be a challenging task for directors. The subject matter can be complex and involve highly technical jargon that is difficult to understand. Companies are also increasing their reliance on emerging technologies and this comes with increased risks. The financial and business impact of a significant cybersecurity breach can be substantial to a company—including an impact on its brand.

Cybermetrics for directors should include information and statistics about digital data and IT systems that can be used to provide effective oversight of IT risks and strategy. Some companies may need to protect IT systems and data that are critical to our nation's infrastructure, like energy and banking. Others may use point-of-sale devices in operations and conduct transactions exclusively on the internet, allow customers and employees to access data via mobile devices, share information with third-party suppliers, or various other activities that can increase cyberrisk. The ideal cybermetric reporting will differ depending on these variables.

There are many other considerations in determining the right cybermetrics to be reported to directors. Factors like the nature of the company's operations (global versus domestic), employee use of mobile devices, the company's leverage of social media and cloud computing, as well as the existing condition of a company's data systems should be considered.

While many boardroom conversations are solely about cybersecurity, the oversight of other aspects of IT operations is also important. For example, the implementation of new systems and the ongoing maintenance of existing systems can lead to system outages that can preclude the company from running its business. So cybermetrics should address a range of topics.

For directors to effectively oversee IT risks, they need the right information in a user-friendly format. But there is no "one size fits all" answer to the level of specifics directors should get. A prescribed list of top cybermetrics that is universally applicable to every company is unrealistic, if not impossible to prepare. Each board needs to work with management to think through which specific information is most valuable in maximizing the effectiveness of their oversight of this challenging area.

A director's fiduciary responsibilities include the duty of care which requires the board to act in "good faith" and exercise the care an ordinary person would use under similar circumstances. When it comes to IT risk oversight, the company's IT-security owner and the board are in a better position to withstand the scrutiny of regulators and plaintiffs if they can provide documentation and clear evidence of governance and accountability; effective risk assessment processes; security programs based on an assessment against a recognized framework; and the monitoring of the progress of the security program and compliance with internal controls. It is also important that the information that the board receives mirrors what the company is asserting to third-parties.

This edition of ACES provides important considerations for directors to determine if they are getting the right cybermetrics delivered in the right way. It addresses the issue by providing insights and leading practices for developing, evaluating, and communicating the appropriate information for effective IT oversight.

Cybermetrics for directors should include information and statistics about digital data and IT systems that are used to provide effective oversight of IT risks and strategy.

2. Who, what, and how is important

Seeing past the haze—Creating clarity and accountability

In order to be effective, audit committees should know who is ultimately accountable from a management perspective for IT risks, including cybersecurity. The responsible corporate officer may be the Chief Information Officer (CIO), CEO, COO, CFO, Chief Risk Officer, or another individual.

In recent years, some companies have designated a Chief Information Security Officer (CISO). This individual generally becomes responsible for establishing and maintaining the company's vision, strategy, and approach to ensure information assets and technologies are adequately protected. A CISO is often established at the corporate level of the company, but companies should give consideration to whether other individuals, particularly at the business-unit level, need to have a similar role that supports the IT-risk owner.

Many companies do not specifically designate a CISO. They choose instead to assign IT security ownership to someone else's existing responsibilities at the company, often making it part of the CIO's responsibilities. Regardless, committees should ensure that someone at the company is responsible for IT security and that this role is documented in his/her job description. This specificity creates a clear understanding of accountability and allows the company to document ownership. Importantly, the responsible individual should have an appropriate role as part of the company's leadership

team and be empowered to lead and make decisions. There has also been a trend of companies establishing a management-level multi-disciplinary cybercommittee to address IT risks across the enterprise, which is led by the individual responsible for IT security. The IT-risk owner is a critical liaison for directors to carry out their oversight responsibilities.

The audit committee will want to decide how often to meet with the responsible corporate officer after considering the company's specific facts and circumstances. Of course, relevant and agreed-upon cybermetrics should be discussed during these meetings. Sixty-five percent of boards are communicating with the company's CIO at least twice a year, including 25% who do so at every formal meeting.[1] The determination of how often to meet should be re-evaluated periodically.

Sometimes it is not what you say, but how you say it

It is common for directors to be frustrated with their interactions with management regarding cybermetrics and IT in general. Many directors cling to a view that IT specialists are too technical and lack effective communication skills.[2] On the other hand, only 21% of directors believe their companies IT strategy and risk approach is very much supported by sufficient understanding of IT at the board level.[3] So, what can directors do to maximize the value of the cybermetric communications they receive?

Audit committees should push management for dialogue that:

- Uses plain English and avoids industry and technical jargon;
- Delivers specific responses to questions versus vague answers;
- Focuses on the "value proposition" of IT security initiatives, expenditures, and proposals;
- Creates a candid dialogue with directors that encourages a discussion of concerns; and
- Presumes that pre-reading materials have been reviewed in advance of the meeting, which allows for a substantive discussion focused on sharing insights versus spending time repeating information already provided.

Audit committees should consider whether they are giving enough input and feedback to presenters to accomplish these objectives. One-on-one meetings outside of formal board meetings with the relevant member of management may be needed to preview proposed board materials and agree on the expectation for effective board communications.

Cybermetric board materials should be easily digestable

Board materials can be overwhelming at times. The sheer volume of information and level of detail provided may exceed what a director really needs to achieve effective oversight. The presentation materials related to IT can easily fall into this trap. It can lead to a director's inability to focus on the key information, which can get lost in the shuffle of so many technical details. There is also a tendency for management to share with directors the same detailed reporting that they receive for their purposes. Such information usually needs to be prioritized and summarized for the directors to be effective.

Prudent audit committees not only play a role in providing input to management about communication practices, but also the way they want to receive cyber information and the frequency of that reporting. Directors should insist on IT risk reporting information that:

- Has an executive summary, allowing for greater focus and understanding of the key issues;
- Highlights significant risk issues upfront, versus burying them in the body of the report;
- Addresses management's perspectives and insights on the IT data, versus simply sharing data;
- Provides easy to understand information in a logical manner—dashboards and graphics can be useful;
- Is circulated well in advance of the meeting, to allow for review; and
- Has been reviewed by senior management before being sent to the board.

The format and content of IT risk materials submitted to the board should be reviewed annually in the interest of continuous improvement.

Audit committees should know who is ultimately accountable from a management perspective for IT risks, including cybersecurity.

[1] PwC, Annual Corporate Directors Survey, 2015.
[2] The CIO Paradox: Battling the contradictions of IT leadership, Martha Heller
[3] PwC, Annual Corporate Director Survey, 2014

Audit committee considerations:

- *Understand which corporate officer is ultimately accountable for IT risks and whether this is documented and well-understood at the company.*
- *Assess whether this individual is sufficiently empowered and part of the leadership team.*
- *Agree on how often to meet and discuss cybersecurity with the responsible individual.*
- *Evaluate whether there is meaningful communication and dialogue regarding IT risks and cybersecurity and provide feedback if the presentation of the materials aren't effective.*
- *Determine whether IT materials presented to the board are prepared in a manner that enhances and maximizes the oversight function and, if not, request changes.*

3. Figuring out the cybermetrics that matter most

Taking a holistic approach

Management should consider addressing cybermetrics in a holistic manner. It is far too common today for companies to narrowly focus on reporting IT risks that are limited to personally identifiable information and the related systems that protect such information. But this is only a part of the discussion that should happen in the boardroom.

Cybermetrics should be considered on a broader level and encompass a company's IT risks beyond just cybersecurity. Why? Today, there is a significant interrelationship between all contributors to overall IT risk, making it difficult to discuss one factor without the others. Certainly cyberattacks can result in a company losing its sensitive intellectual property or directly impact its brand. But, a company's integrated "value chain," consisting of suppliers and distributors that are digitally connected, can exacerbate these cyber risks. And the era of the "internet of things" creates a greater level of connectivity with a company's digital data, including mobile devices, cloud computing, big data, social media, point-of-sale devices, and other technologies. Add to this, companies need to invest for the future and consider how technological innovation can change their business model or create the risk of becoming obsolete.

Some boards may only focus on cyber risks in a reactive manner, involving a focus on hindsight, including receiving information regarding successful hacks, failed attempts, or compromised accesses. These events get a lot of attention. While it is important to understand the company's history of cyberattacks, it is also critical to focus on preventative actions and ensure that the cybermetrics reported to the board allow directors to understand how the risks of penetration are mitigated.

Beyond the interrelationship of IT risks with strategy and operations, a holistic approach to the reporting of cybermetrics can result in a comprehensive view of the IT risk universe, providing more valuable and effective information to directors. This is consistent with common stakeholder expectation that directors have broader IT oversight. Further, it may be challenging for directors to understand the full IT risk landscape if they receive information exclusively on cybersecurity and then receive a separate report about IT risks and strategy that are integral to a company's operations.

Baseline information the board must know

All directors overseeing IT must understand and have a reference point related to current aspects of a company's IT and security environment. This information should be agreed upon between management and the board.

Baseline information can cover a variety of aspects of the company's IT systems, including areas like:

Protections over the "crown jewels." An understanding of the 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. It also includes sensitive information the company has custody of, for example, customer credit card information, health care records, and customer and employee financial information. Relevant baselining cybermetrics data should be focused on protecting these digital assets.

Coverage by a cyberinsurance policy. Directors should understand the company's position on cyberinsurance coverage, and if applicable, what the policy covers (and, more importantly, what it doesn't cover), levels of coverage, policy limits, and other relevant matters. It can be useful to understand how a company's policy benchmarks against other companies, particularly in its industry. Cyberinsurance is a nascent an evolving industry, making it more important that companies thoroughly understand their policies.

Identification of needed IT upgrades. When companies delay discretionary software upgrades or replacing legacy IT infrastructure—"deferred IT maintenance"—it can create greater risk. Knowing which of the key digital systems have not been updated can be a useful baseline cybermetric. Also, testing the company's ability to recover mission-critical systems in the event of a failure is important.

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 presecribed framework or a one-size-fits-all solution addressing an effective structure. Directors should have baseline information about their company's cybersecurity program and how it compares to a specific framework. Such frameworks can include: the Commerce Department's National Institute of Standards and Technology Cybersecurity Framework ("NIST Framework"), ISO 3100: Risk Management – Practices and Guidelines, COSO: Enterprise Risk Management – Integrated Framework, and ISACA frameworks of COBIT 5.

The NIST Framework is a newly-introduced framework. It has received publicity for a number of reasons, including being developed under Executive Order by President Obama. This framework presents companies with a voluntary methodology to implement and evaluate cyber controls and could establish a de facto standard to which companies may be held accountable, including by plaintiffs' counsel. The NIST Framework may even be employed by specialized cyberinsurance companies when determining risks and premiums for issuing new policies.

Regardless of the framework utilized, companies should assess its current cyber status against it and report the results to the board. This reporting can be included in the board's cybermetric package at the appropriate level of detail at an agreed-upon frequency, and may take the form of a "heat chart." For example, the NIST framework breaks cybersecurity into five basic functions – Identify, Protect, Detect, Respond, and Recover. The reporting could use a rating, for example, color-coding or a numeric ranking, for each function and category to signify the degree of compliance with the guidance in the framework. Through this process, an audit committee can understand gaps between their company's current and desired cyber state, progress or regress in each area, and evaluate the action plan to improve the company's cyber stature. This information should be periodically updated for directors as circumstances change.

Status of IT "health." Baseline information should include benchmark data related to budgeted and actual security investments made by the company compared to industry/peers. It is also important for companies to assess and boards to know the company's actual level of cyberspend compared to budget and the level of "shadow IT" costs (i.e., costs incurred outside the control of the CIO by the business units).

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] This situation makes preventative employee cybersecurity training an important information for the board.

Additional"menu" of possible cybermetrics

Beyond simply receiving baseline information, directors will want to consider a number of additional metric candidates dealing with digital data. Certainly, not all metrics are relevant to every company and must be prioritized for each board. The following are examples to consider:

Systems infrastructure:

- Percentage of the infrastructure and network assets covered by real-time monitoring and alerting
- Results of the company's systems' scanning, including detected and remediated spyware and malware
- Level of unplanned down-time due to security incidents and IT outages
- Percentage of "masked," "data fragmentation," or "tokenization" implemented for sensitive data implemented
- Results of penetration testing conducted at the company
- Number of stolen log-in credentials identified
- Number of successful security breaches and the "mean time-to-incident" detection and recovery
- Results of internal and external auditors testing of IT security controls, noting that the responsibilities of the external auditors is limited to IT controls that impact financial reporting
- Disciplinary and corrective actions taken as a result of violations
- Results of "tabletop" IT recovery exercises, including live tests of data center failovers and individual systems failovers

Third-parties:

- Third-party providers with access to the company's "crown jewels"
- Level of third-party participation in the company's IT compliance program
- Number of security access violations by third-parties

Mobile computing:

- Number of employees using bring-your-own-device (BYOD) to access company data

[4] PwC, The Global State of Information Security Survey 2015

- Level of adherence to the company's BYOD policies
- Percentage of employees trained on cyber policies and practices related to mobile devices
- Number of authorized and unauthorized mobile devices accessing IT systems
- Results of testing to identify unauthorized devices gaining access to company data
- Percentage of data used via mobile devices that is protected by encryption technology
- Percentage of employee devices subject to remote "wiping" when lost or stolen

Big Data:
- Status of data capture and analysis activities impacting company's strategy
- Efficiency in converting raw data into usable and relevant information to improve operations
- Trends identified as a result of data capture activities impacting company's strategy
- Return on investment for current use of data analytics
- Competitor usage of big data analytics

Social media:
- Number of followers on company social media sites
- Percentage of employees trained on cyber policies and practices related to social media
- Level of compliance with existing regulations around social media
- Number of negative publicity postings about the company on social media

Cloud computing:
- Number of providers used for enterprise cloud services
- Cost of cloud services compared to the typical "run rate" of the IT department
- Percentage of data accessible via cloud services that is protected by encryption technology
- Status of backup plans for business continuity if the company's cloud service goes down

IT security for international travel
- Violations for international travelers without appropriate security features for travel, like the inability to update software while travelling and use of the company's virtual private network to access email
- Percentage of independent secure email accounts that are used for international travelers
- Compliance with the company's overall IT policies when travelling internationally

In summary, directors should ask for cybermetrc data that:

- Considers the top 10 or 15 metrics that are critical to keep focus on the most significant areas;
- Delivers a holistic picture of the company's IT risks;
- Connects to the company's strategic goals and shows management's progress in achieving those goals;
- Uses proactive and leading measures in addition to lagging and reactive measures;
- Provides context for directional changes through the use of agings, rankings, or other trend information to facilitate reviews and share insight on data; and
- Is relevant to the company's particular situation.

Beyond the interrelationship of IT risks with strategy and operations, a holistic approach to the reporting of cybermetrics can result in a comprehensive view of the IT risk universe, providing more valuable and effective information to directors.

Audit committee considerations:

- *Evaluate whether the cybermetrics being presented to the directors enhance and maximize the oversight function.*
- *Ask whether management took a holistic view of IT risks beyond basic cybersecurity when considering cybermetric reporting to directors.*
- *Evaluate baseline metrics to understand the company's current cyber and IT environment and the gaps to achieving its desired cyber state.*
- *Discuss and agree on the prioritization of the most important metrics, with a focus on the top 10 or 15.*

4. It's a changing world and a continuous process

It is essential that the reporting of cybermetrics to the board is updated and reevaluated periodically. Given the pace of change for IT and the increased sophistication of hacking, reporting cannot be a one-time exercise and has to be an ongoing effort.

Cybermetrics must be revised as the company matures, faces new difficulties, uses new technology, or is involved

in a major event like a merger and acquisition. There may also be changes in the cybersecurity environment, including laws and regulations that need to be evaluated and potentially reflected in the company's cybermetric reporting. Another area to re-evaluate periodically is the frequency of discussions about IT risks between directors and the responsible corporate officer.

Audit committee considerations:

- *Continue to regularly re-evaluate the cybermetric reporting to directors, updating it for changes in the company's maturity, circumstances, and current cyber environment.*
- *Consider the impact of changes to the company's operating environment and broader cyber community on current cybermetric reporting; consider whether any changes are necessary.*

How PwC can help

To have a deeper discussion about how this topic might impact your business, please contact your engagement partner or one of the individual's noted below:

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

Catherine Bromilow
Partner, Center for Board Governance
(973) 236 4120
catherine.bromilow@us.pwc.com

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

Charles Beard
Principal, Forensic Services
(703) 918-3318
charles.e.beard@us.pwc.com

Grant Waterfall
Partner, Cybersecurity and Privacy
(646) 471-7779
grant.waterfall@us.pwc.com

Other topics

Other "Audit Committee Excellence Series" topics include:

- Assessing the company's forward-looking guidance practices and the potential risks of consensus estimates (March 2014)
- Financial reporting oversight (May 2014)
- Overseeing internal audit (July 2014)
- Overseeing external auditors (September 2014)
- Overseeing accounting changes—including the new revenue recognition standard (February 2015)
- Role, composition, and performance (May 2015)
- Dealing with investigations (June 2015)

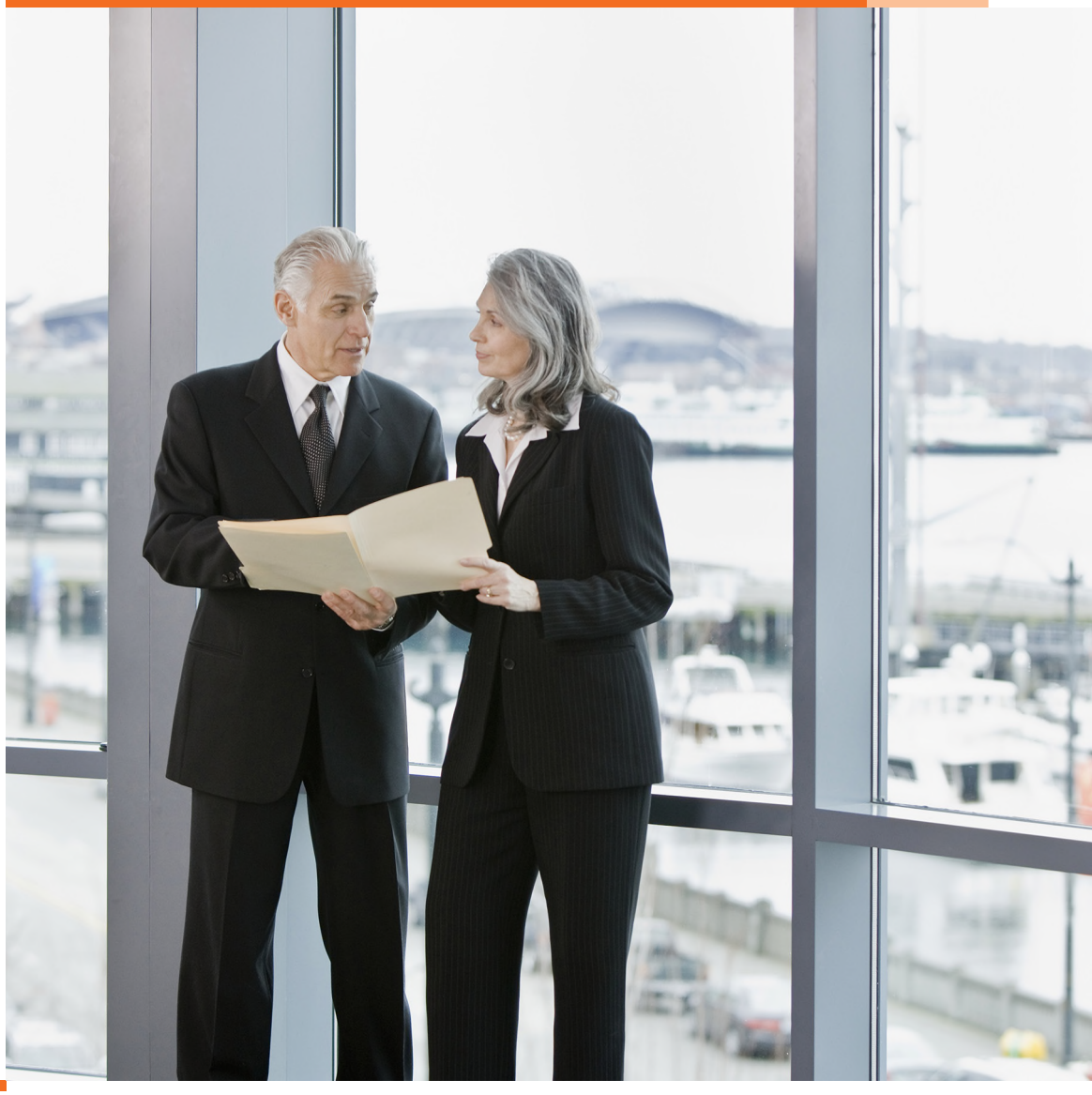
Find more information at www.pwc.com/us/CenterforBoardGovernance

Download our iPad app at www.pwc.com/us/BoardCenterApp

Appendix C: PwC Annual Corporate Directors Survey - The gender edition

PwC's 2014 Annual Corporate Directors Survey -
The gender edition

May 2015



pwc

Table of contents

Please note: Charts may not all add to 100 percent due to rounding

Introduction

The global discussion about gender diversity on public company boards continues. In addition to the adoption of quotas in several countries, a number of organizations in the US have undertaken significant efforts to increase the gender diversity of directors. Despite this, the number of women serving as directors has not changed significantly over the last six years (18% of all S&P 500 directors are now female compared to 16% in 2008[1]). Additionally, a number of academic studies have recently been published attempting to prove or disprove a causal relationship between gender diversity on boards and company performance.

Within this context, there are two fundamental questions about gender representation and director performance that deserve to be asked: Are there really differences in how male and female directors approach their oversight roles? And, do the practices of boards with female directors vary from those of other boards? This report addresses these questions by looking at what male and female directors told us about their individual perspectives and the boards on which they serve.

During 2014, 863 public company directors responded to PwC's 2014 Annual Corporate Directors Survey. Of those directors, 70% serve on the boards of companies with more than $1 billion in annual revenue. Participants were 86% male and 14% female—closely aligning with gender distribution averages of Fortune 500 public company directors. The board tenure of participants was relatively even. While participants came from nearly two dozen industries, the leading sectors represented included industrial products, banking and capital markets, and technology. Participants were asked to respond about only the largest board on which they serve.

Our survey findings show that male and female directors clearly do have different perspectives on some important corporate governance issues. And in some areas, practices differ for boards that have female director representation. In particular:

- **Women are far more likely to consider board diversity important.**
- **Women see more obstacles to replacing an underperforming director and are more likely to believe their board evaluation process could be enhanced.**
- **Women say their boards have adopted more of the governance structures or practices viewed as "leading" by certain stakeholders.**
- **Both men and women are concerned about director-shareholder communications, but male director concerns are deeper.**
- **Women want to spend more time on IT despite higher levels of engagement, and are more concerned about the digital skills of today's boards.**
- **Women expect more when it comes to board materials**

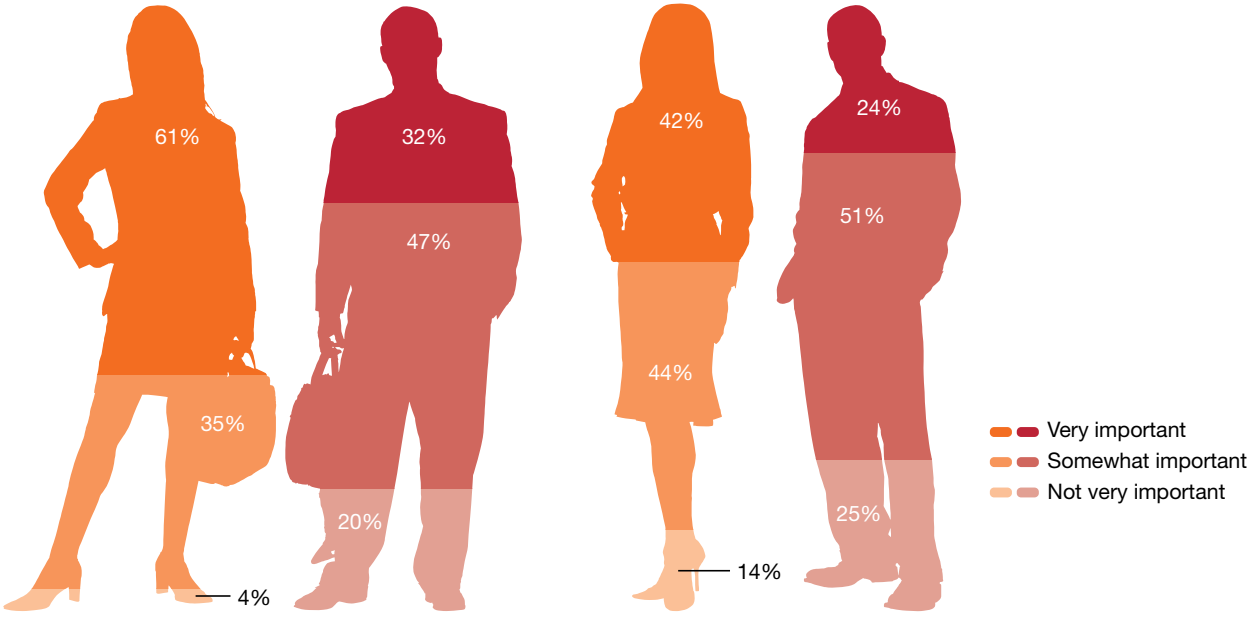
Regardless of the differences in views among male and female directors, current trends point to an evolution that will likely impact gender diversity on future boards. Fortune 50 female directors tend to be younger, with an average age of 60—compared to 63 for males[1]. Additionally, 24% of all new S&P 500 directors named in the last two years have been women[1]—compared to the current 18% ratio of women to men. And, in general, male directors have been on their boards longer. Considering these factors, it's reasonable to project that the board of the future will include a higher proportion of women than today's boards.

1 *Spencer Stuart U.S. Board Index 2014*

Perspectives on the need for diversity

Male and female directors disagree about the importance of having gender and racial diversity on their boards. Female directors are far more likely to consider board diversity to be important. For example, 61% of female directors describe gender diversity as "very important" compared to 32% of male directors. Similarly, 42% of female directors describe racial diversity as "very important," compared to 24% of their male counterparts. While fewer than one-in-five directors say their board has recruited new directors with diverse backgrounds over the last 12 months, 57% say they are talking about doing so going forward.

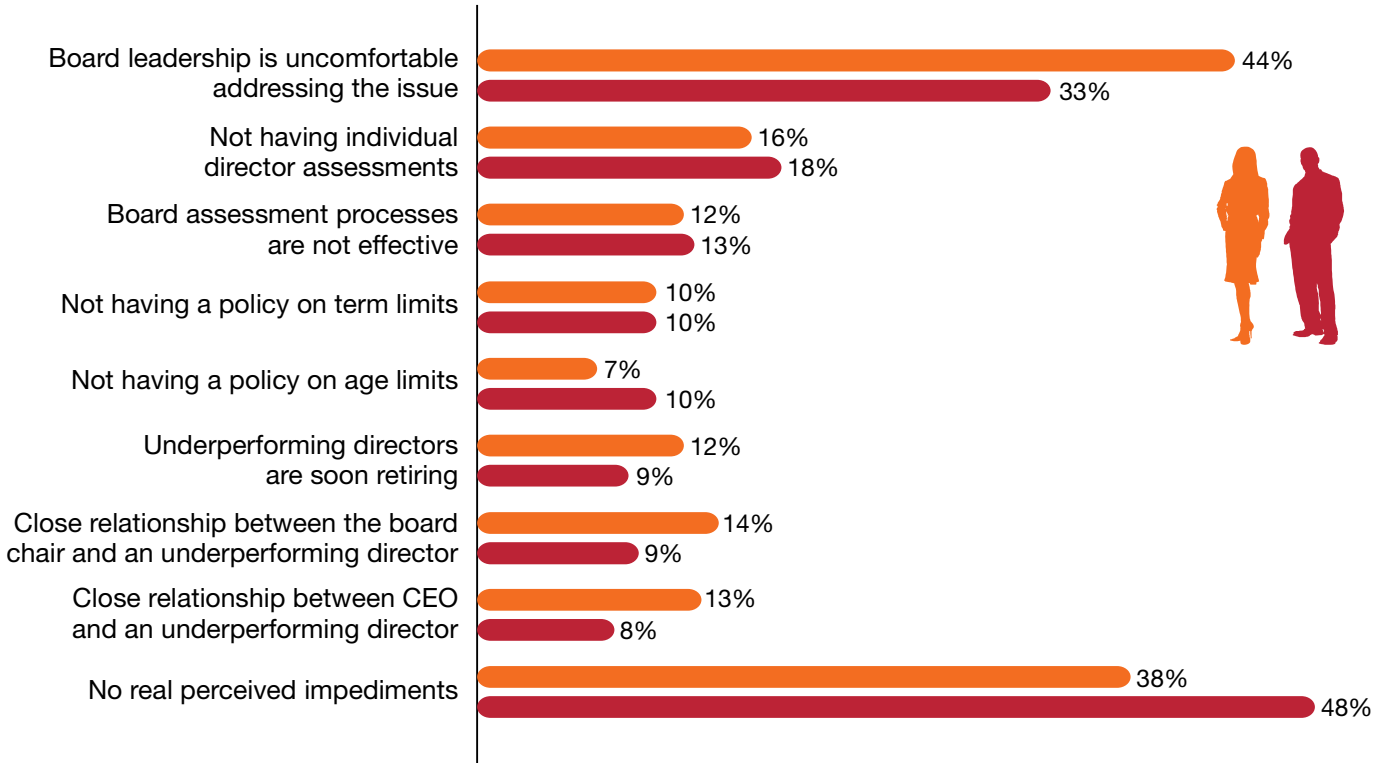
How would you describe the importance of having the following on your board?



Impediments to board renewal

While director dissatisfaction with peer performance grew in 2014, so did the percentage of directors who recognize impediments to replacing underperforming fellow directors (53% compared to 48% in 2013). Female directors are ten percentage points more likely than male directors to believe there are impediments to replacing an underperforming director. When it comes to identifying specific impediments, female directors are eleven percentage points more likely to blame board leadership for their board's inability to replace an underperforming director. Female directors also more frequently cite close relationships between the underperforming director and the board chair and the CEO as impediments to board renewal.

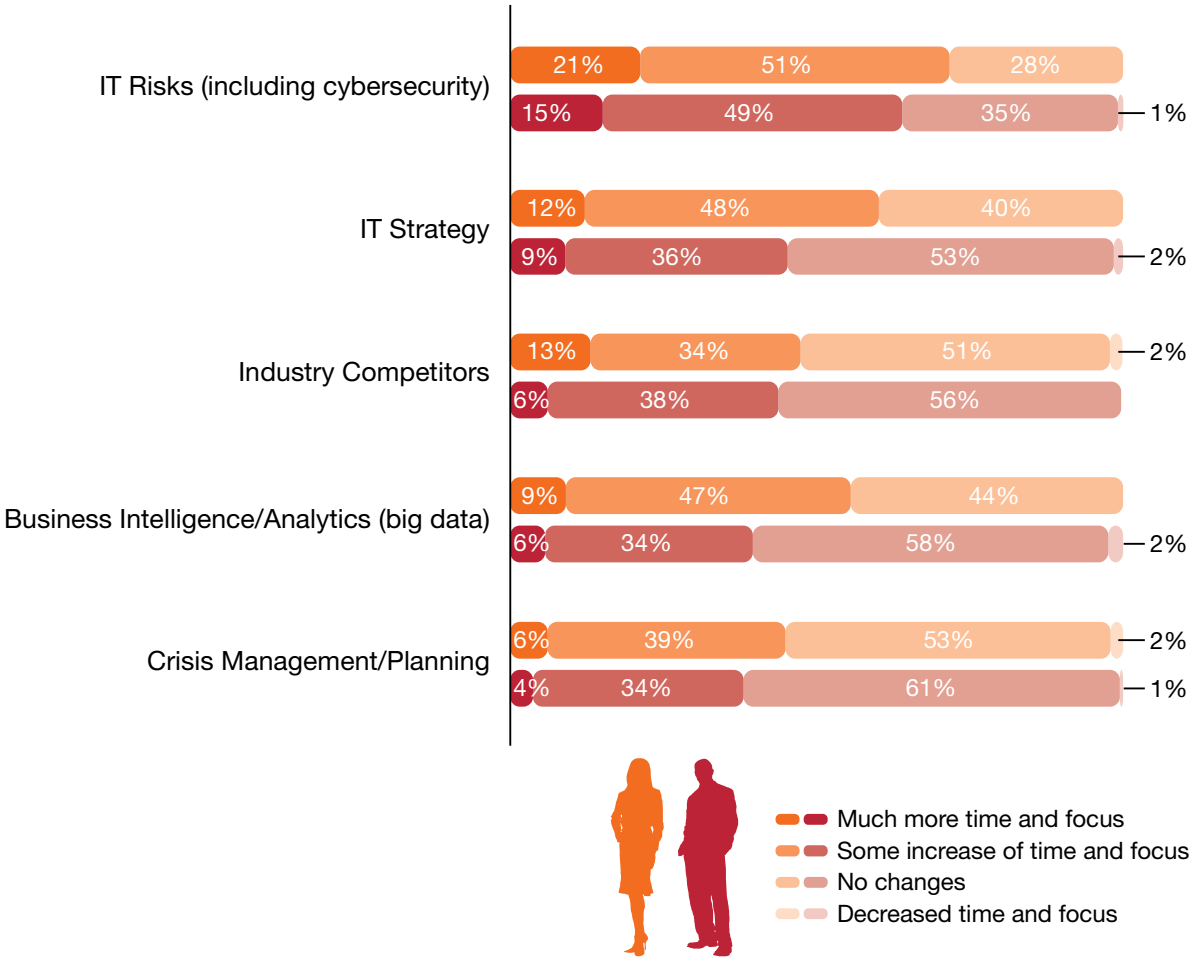
What are the impediments to replacing an underperforming director?



Do men and women want to prioritize the same issues?

The average time commitment of public company directors continues to increase (now 242 hours per year[2]) due to a variety of factors. Even so, many directors express a desire to dedicate additional time to certain areas. In particular, female directors want more time and focus on IT issues than male directors: 60% want an increase of time and focus on IT strategy (compared to 45% of men). And, 72% of females want at least "some" additional focus on IT risks like cybersecurity (compared to 64% for men); 56% want more attention given to big data (compared to 40% for men). Female directors also want to spend more time than males in other areas including the discussion of industry competitors and crisis management planning.

Please indicate if you believe your board should change the amount of time it spends on:

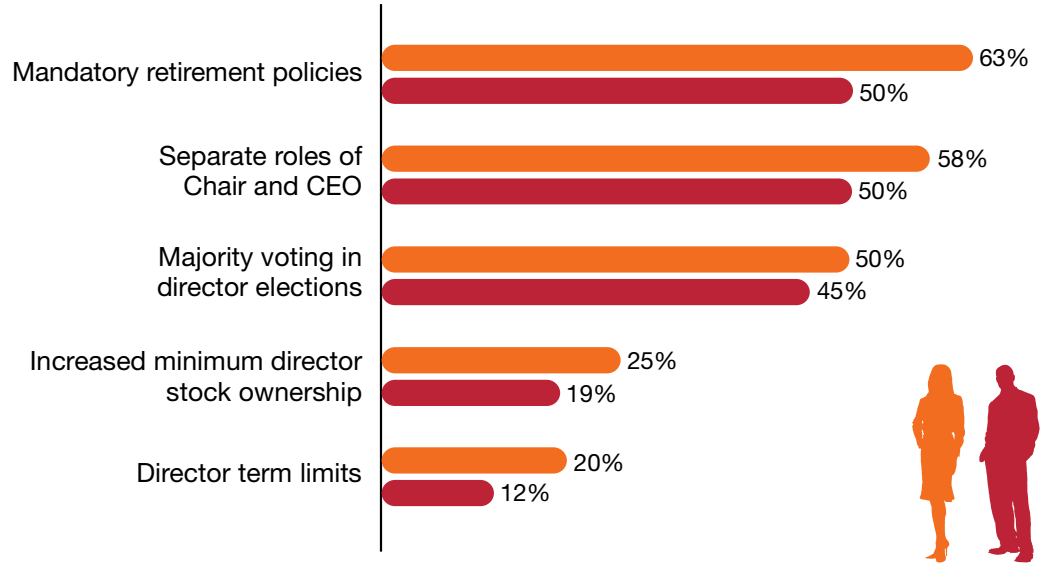


2 *NACD 2014 Public Company Governance Survey*

Thoughts about leading governance initiatives

Female directors indicate that a greater percentage of their boards have adopted some of the governance structures or practices viewed as "leading" by certain stakeholders. For example, 63% of females say their board has adopted mandatory retirement policies, compared to only half of male directors. Similarly, 58% of females say their board has separated the roles of Chair and CEO compared to only half of males. Female directors also indicate that a higher percentage of their boards have adopted term limits and majority voting in director elections.

Percentage of directors indicating their board has already adopted the following:



Women directors are more skeptical of their board evaluation process

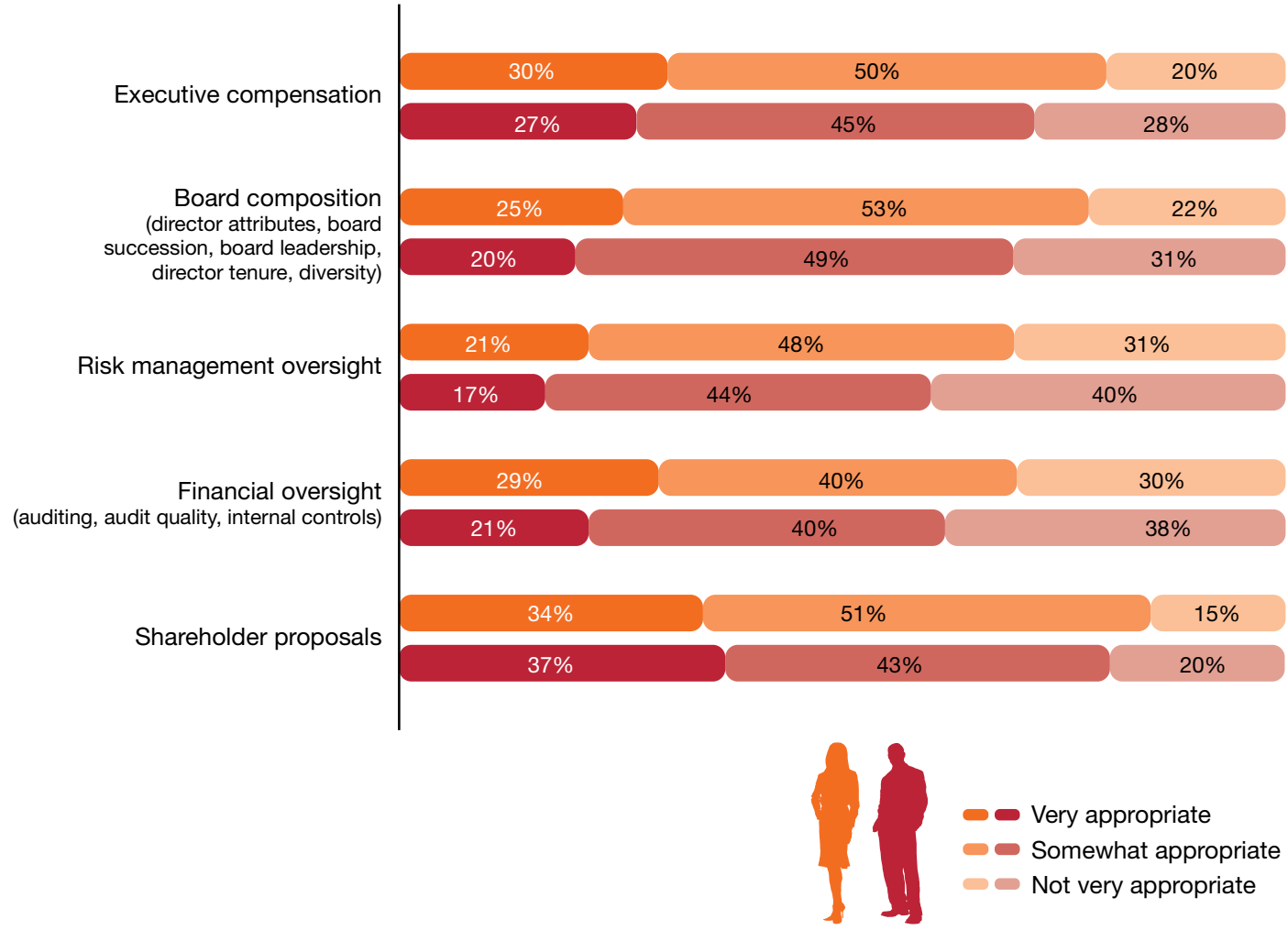
An effective board and committee self-evaluation process can be a critical tool in achieving board effectiveness. The vast majority of all directors view their self-evaluations favorably—with over 90% believing their self-evaluation processes are at least "somewhat effective." However, women are more likely to believe their board evaluation process can be enhanced. Nearly a quarter of female directors characterize their board leadership as "not at all effective" in leading the process, compared to only 12% of male directors. Additionally, female directors are less likely to believe there is sufficient follow-up after the self-evaluation process.

Regarding board/committee self-evaluations, to what extent do you believe:

Which directors want to talk?

Director communications with stakeholders increased across many constituencies in 2014. A greater percentage of directors are communicating with institutional investors—67% now say their board does so compared to 62% in 2013. However, there are different views among male and female directors on the appropriateness of direct dialogue on particular topics. Female directors are more likely than male directors to view discussions with investors about risk management oversight as appropriate (69% versus 60%). Additionally, female directors view executive compensation, board composition, financial oversight, and shareholder proposals as more appropriate topics for direct dialogue than male directors.

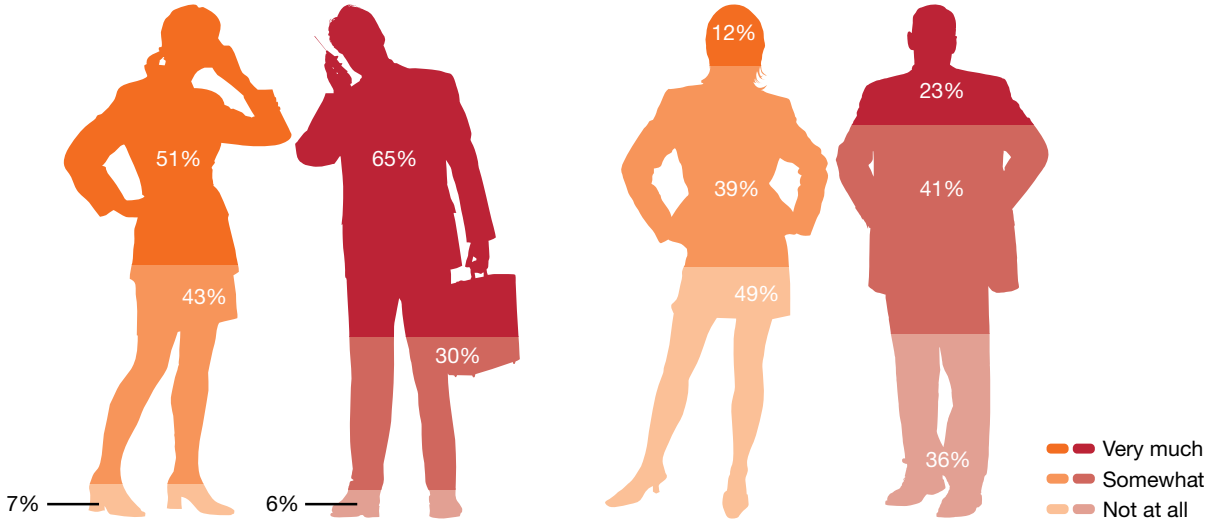
Regarding the following topics, how appropriate is it for boards to engage in direct communications with shareholders?



Communication risks worry men

Many directors have historically been reluctant to participate in direct communications with shareholders for a variety of reasons, including the risk of having too many voices speaking on behalf of the company, concern that investors have special agendas, and worries about violating Regulation Fair Disclosure. Overall, male directors are more likely to express trepidation about such communications; 65% believe "very much" that it creates too great a risk of mixed messages compared to 51% of female directors. And, 23% of male directors don't believe it's appropriate to communicate directly with shareholders on any topic—compared to just 12% of female directors.

To what extent do you agree with the following regarding director/shareholder communications:



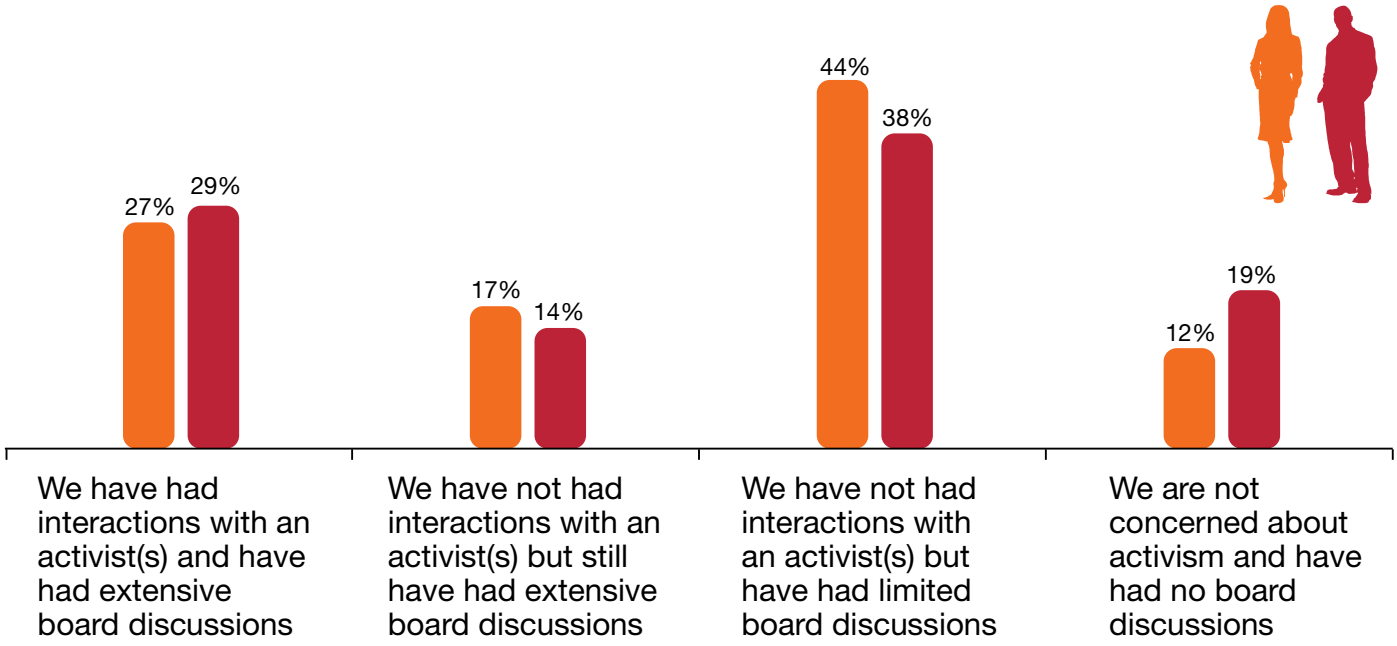
Director communications create too great a risk of mixed messages (different people speaking on behalf of the company)

It is not appropriate to engage directly with investors on any subject

Preparing for shareholder activism

The shareholder activism environment has intensified over the last several years and activist investors now have more than $100 billion in assets under management. Director experience confirms this, as about one in four directors interacted with activists and held extensive board discussions about activism in the last year. A greater percentage of female directors have had extensive or limited board discussions about activists despite having no interaction. And, only 12% of women are not concerned about activism compared to 19% of males.

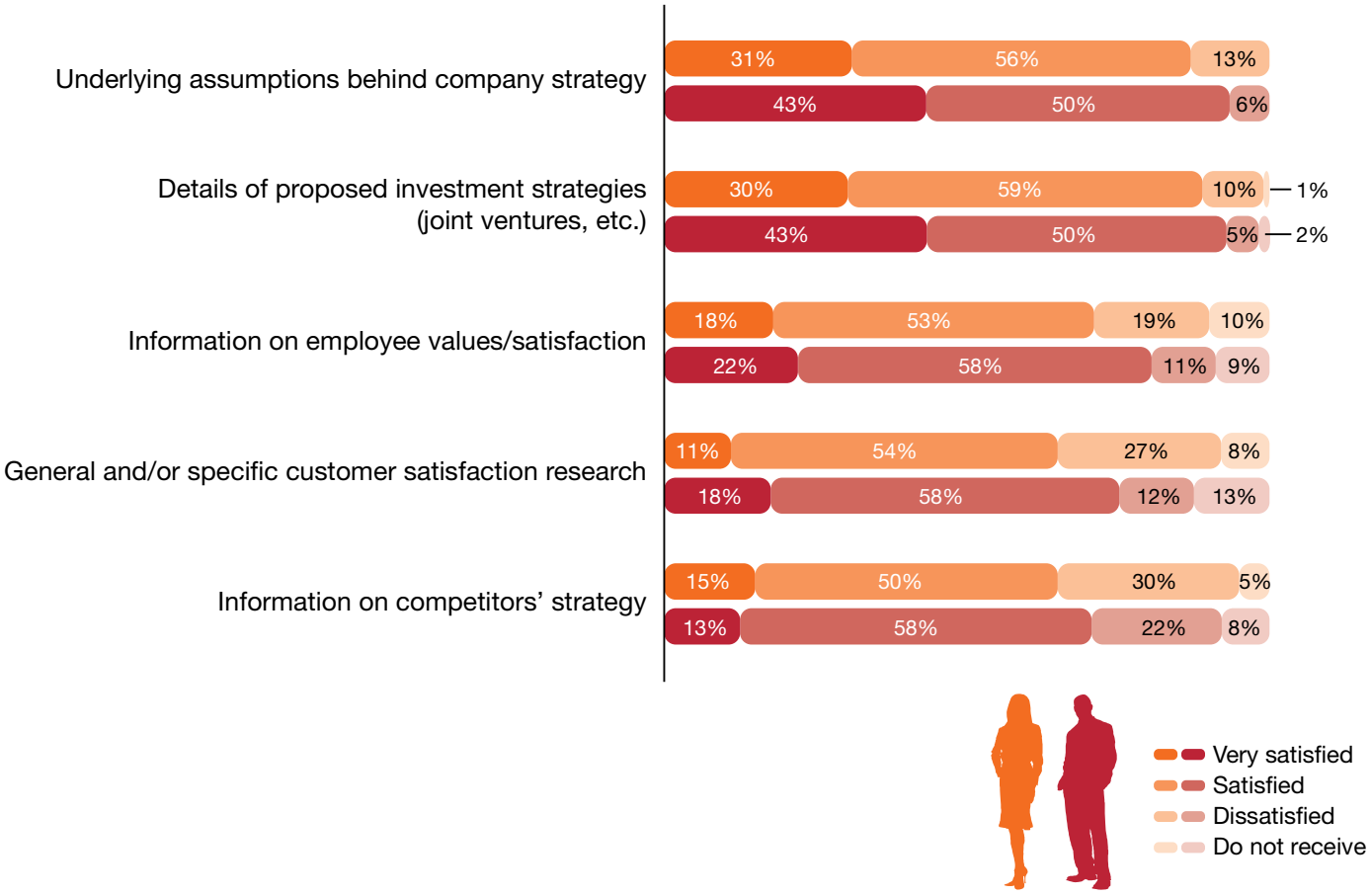
How would you describe your board's preparation for and actual experience with shareholder activism?



Am I getting what I want?

On the whole, directors are pleased with the strategic information they receive from management. However, female directors expect more when it comes to board materials. For example, 43% of male directors are "very satisfied" with the information they are given regarding the underlying assumptions behind company strategy, compared to only 31% of female directors. And female directors are more than twice as likely to say they are "dissatisfied" with this strategic information. Additionally, female directors are less satisfied with the information they receive on customer satisfaction research, employee satisfaction, competitor strategy, and details of proposed investment strategies.

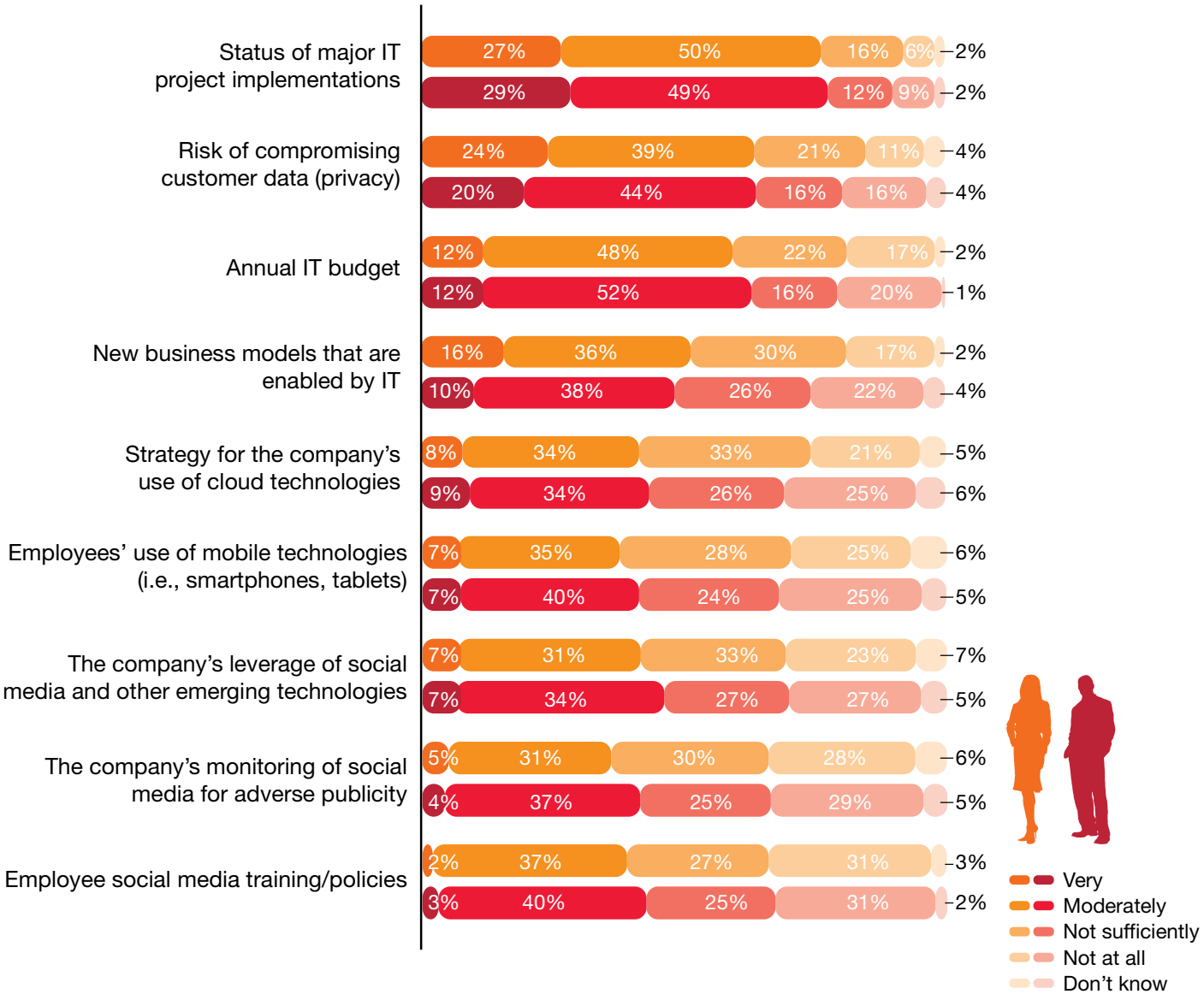
How satisfied are you with the following information provided to your board?



Women focus on IT issues

Director engagement with IT topics increased from 2013, but in nearly every IT area, a greater percentage of female directors describe their board or its committees as "not sufficiently" engaged. This was particularly true about the level of engagement regarding the company's cloud strategy, leverage of social media, privacy, new business models enabled by IT, and the annual IT budget.

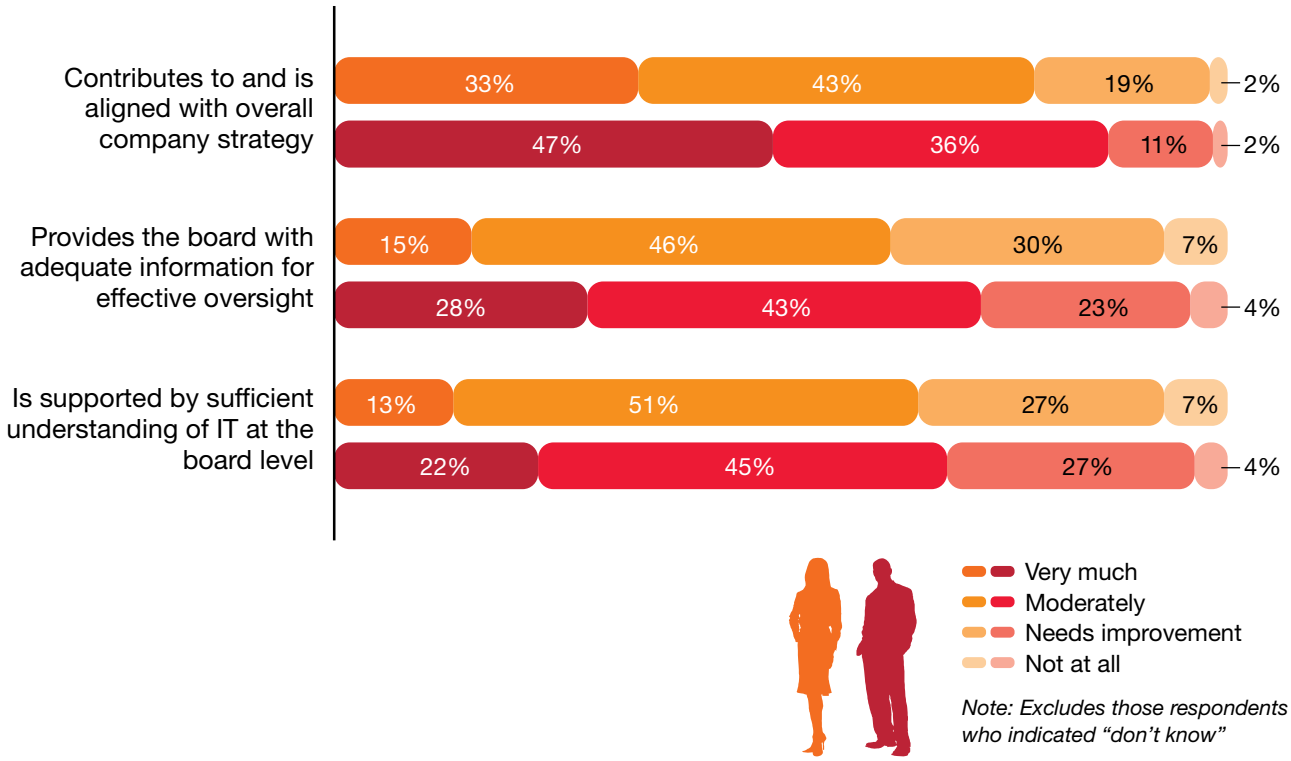
How engaged is your board or its committees with overseeing/understanding the following?



Confidence in IT oversight capabilities

Overall, female directors are less confident than males with their company's approach to IT strategy and IT risk mitigation. Female directors are fourteen percentage points less likely to believe their company's IT strategy and IT risk mitigation approach "very much" contributes to and is aligned with the overall company strategy. Only 15% of female directors "very much" believe the company's IT strategy and IT risk mitigation approach provides the board with adequate information for effective oversight—compared to 28% of male directors. Female directors are also less likely than males to believe the company's approach to IT strategy and IT risk mitigation is "very much" supported by a sufficient understanding of IT at the board level.

Do you believe your company's IT strategy and IT risk mitigation approach:

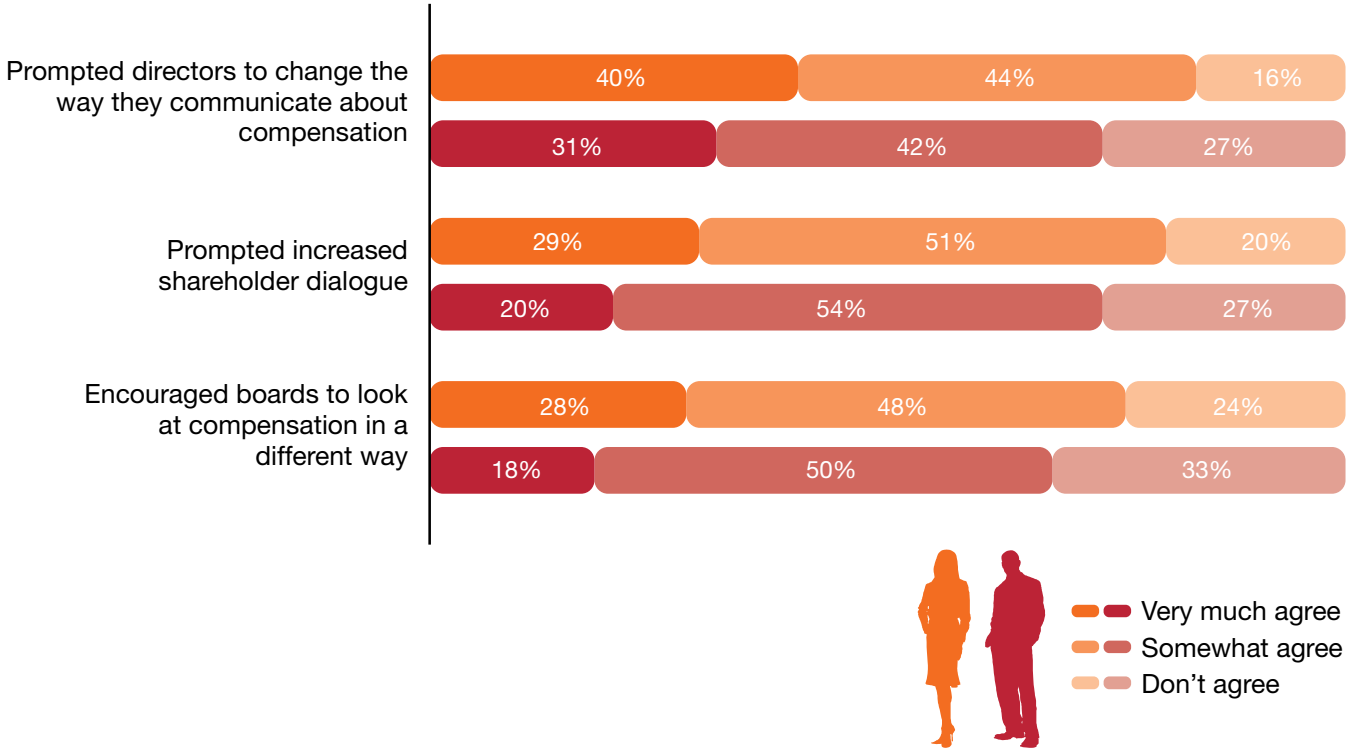


Note: Excludes those respondents who indicated "don't know"

Men less positive about "say-on-pay"

Female directors are more likely than males to believe that say-on-pay voting had a significant cumulative impact on evaluating compensation and related communications. For example, 28% of female directors believe say-on-pay encouraged their board to look at compensation in a different way—but only 18% of male directors feel the same way. Additionally, a greater percentage of women believe that say-on-pay prompted directors to change the way they communicate about compensation. Both genders generally believe it prompted increased shareholder dialogue.

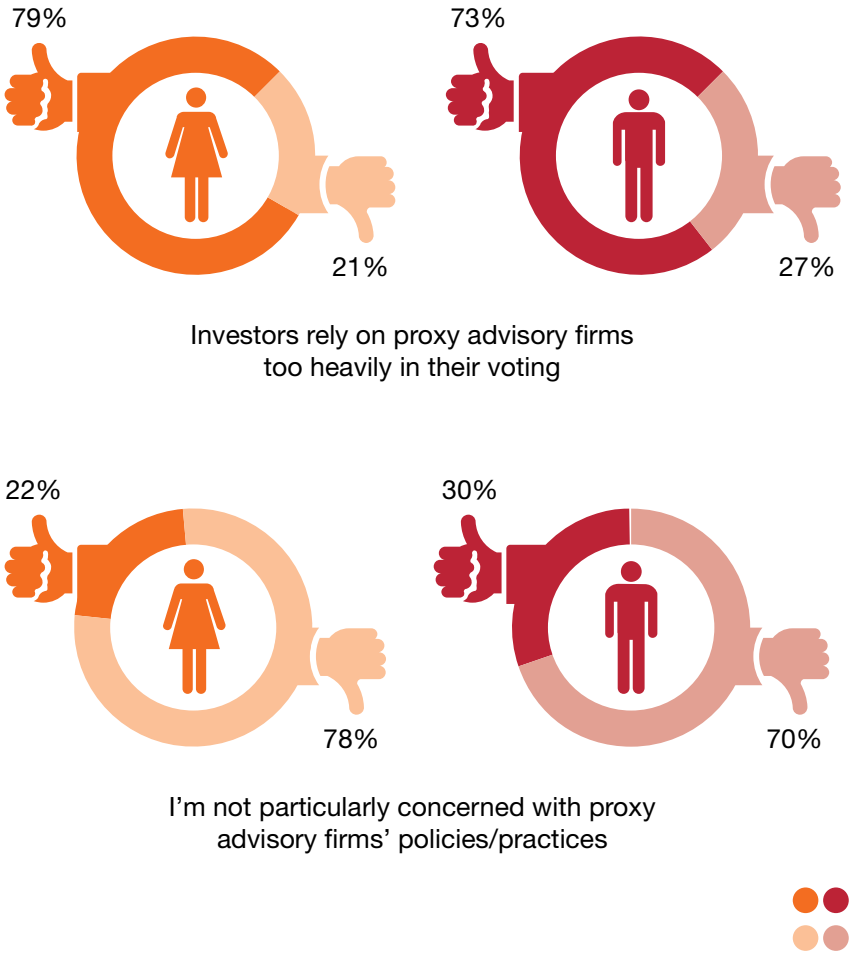
What is your assessment of the cumulative impact of "say-on-pay" voting?



Shared concerns about proxy advisory firms

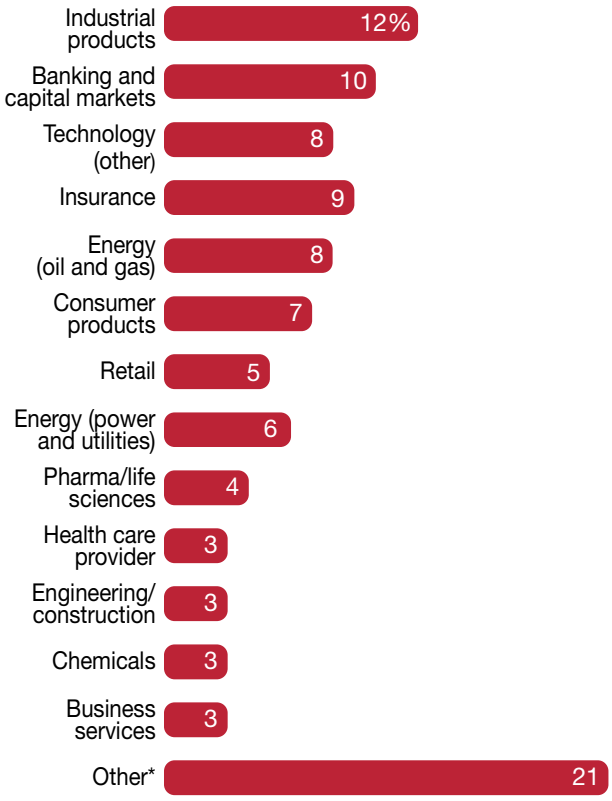
While both male and female directors express significant concern with the policies and practices of proxy advisory firms, female directors are six percentage points more likely to believe that investors rely on proxy advisors too heavily in their voting decisions.

Which of the following concerns do you have with proxy advisory firms:



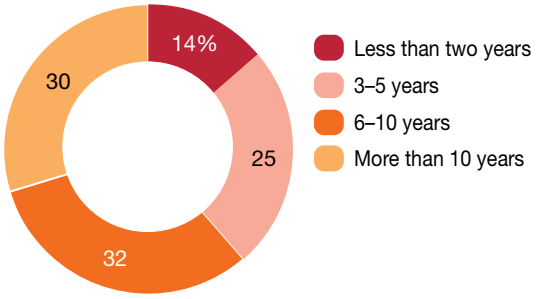
Demographics of survey participants

Which of the following best describes the company?

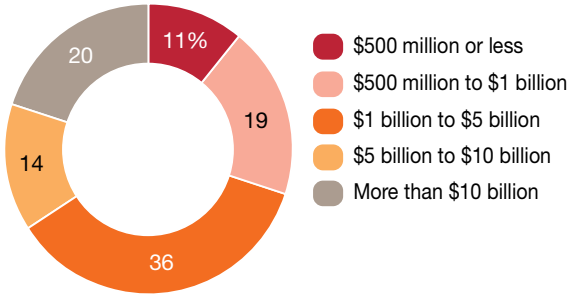


*Other includes the sum of the following industries with no individual response receiving over 2%: transportation/logistics; software/internet solutions; semiconductor; hospitality/leisure; government contracting; communications; automotive; asset management; mining; healthcare payer; forest, paper, and packaging; entertainment/media; and agribusiness.

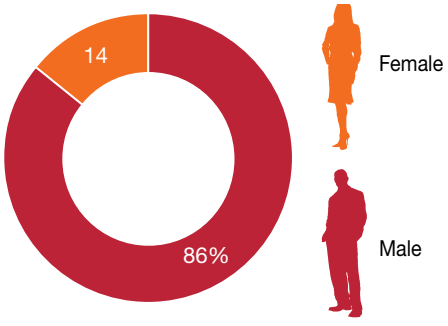
How long have you served on this board?



What are the annual revenues of the company?



You are:



www.pwc.com

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

Mary Ann Cloyd
Leader, Center for Board Governance
PwC
(973) 236 5332
mary.ann.cloyd@us.pwc.com

Paula Loop
Incoming Leader, Center for Board Governance
PwC
(646) 471 1881
paula.loop@us.pwc.com

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

Paul DeNicola
Managing Director, Center for Board Governance
PwC
(973) 236 4835
paul.denicola@us.pwc.com