Harvard Business Review
www.hbr.org

Board practices for monitoring technology investments vary widely and often wildly. As technology's cost, complexity, and consequences grow, directors need a framework to develop IT policies that fit the companies they oversee.

Information Technology and the Board of Directors

by Richard Nolan and F. Warren McFarlan

Reprint R0510F

Board practices for monitoring technology investments vary widely and often wildly. As technology's cost, complexity, and consequences grow, directors need a framework to develop IT policies that fit the companies they oversee.

Information Technology and the Board of Directors

by Richard Nolan and F. Warren McFarlan

Ever since the Y2K scare, boards have grown increasingly nervous about corporate dependence on information technology. Since then, computer crashes, denial of service attacks, competitive pressures, and the need to automate compliance with government regulations have heightened board sensitivity to IT risk. Unfortunately, most boards remain largely in the dark when it comes to IT spending and strategy. Despite the fact that corporate information assets can account for more than 50% of capital spending, most boards fall into the default mode of applying a set of tacit or explicit rules cobbled together from the best practices of other firms. Few understand the full degree of their operational dependence on computer systems or the extent to which IT plays a role in shaping their firms' strategies.

This state of affairs may seem excusable because to date there have been no standards for IT governance. Certainly, board committees understand their roles with regard to other areas of corporate control. In the U.S., the audit committee's task, for example, is codified in a set of Generally Accepted Accounting Principles and processes and underscored by regulations such as those of the New York Stock Exchange and Securities and Exchange Commission. Likewise, the compensation committee acts according to generally understood principles, employing compensation consulting firms to verify its findings and help explain its decisions to shareholders. The governance committee, too, has a clear mission: to look at the composition of the board and recommend improvements to its processes. To be sure, boards often fail to reach set standards, but at least there are standards.

Because there has been no comparable body of knowledge and best practice, IT governance doesn't exist per se. Indeed, board members frequently lack the fundamental knowledge needed to ask intelligent questions about not only IT risk and expense but also competitive risk. This leaves the CIOs, who manage critical corporate information assets, pretty much on their own. A lack of board oversight

for IT activities is dangerous; it puts the firm at risk in the same way that failing to audit its books would.

Understanding this, a small group of companies has taken matters into its own hands and established rigorous IT governance committees. Mellon Financial, Novell, Home Depot, Procter & Gamble, Wal-Mart, and FedEx, among others, have taken this step, creating board-level IT committees that are on a par with their audit, compensation, and governance committees. When the IT governance committee in one of these companies assists the CEO, the CIO, senior management, and the board in driving technology decisions, costly projects tend to remain under control, and the firm can carve out competitive advantage.

The question is no longer whether the board should be involved in IT decisions; the question is, how? Having observed the ever-changing IT strategies of hundreds of firms for over 40 years, we've found that there is no one-size-fits-all model for board supervision of a company's IT operations. The correct IT approach depends on a host of factors, including a company's history, industry, competitive situation, financial position, and quality of IT management. A strategy that works well for a clothing retailer is not appropriate for a large airline; the strategy that works for eBay can't work for a cement company. Creating a board-level committee is not, however, a best practice all companies should adopt. For many firms—consulting firms, small retailers, and book publishers, for instance—it would be a waste of time.

In this article, we show board members how to recognize their firms' positions and decide whether they should take a more aggressive stance. We illustrate the conditions under which boards should be less or more involved in IT decisions. We delineate what an IT governance committee should look like in terms of charter, membership, duties, and overall agenda. We offer recommendations for developing IT governance policies that take into account an organization's operational and strategic needs, as well as suggest what to do when those needs change. As we demonstrate in the following pages, appropriate board governance can go a long way toward helping a company avoid unnecessary risk and improve its competitive position.

The Four Modes

We've found it helpful to define the board's involvement according to two strategic issues: The first is how much the company relies on cost-effective, uninterrupted, secure, smoothly operating technology systems (what we refer to as "defensive" IT). The second is how much the company relies on IT for its competitive edge through systems that provide new value-added services and products or high responsiveness to customers ("offensive" IT). Depending on where companies locate themselves on a matrix we call "The IT Strategic Impact Grid" (see exhibit), technology governance may be a routine matter best handled by the existing audit committee or a vital asset that requires intense board-level scrutiny and assistance.

Defensive IT is about operational reliability. Keeping IT systems up and running is more important in the company's current incarnation than leapfrogging the competition through the clever use of emerging technology. One famously defensive firm is American Airlines, which developed the SABRE reservation system in the late 1960s. Once a source of innovation and strategic advantage, the SABRE system is now the absolute backbone of American's operations: When the system goes down, the airline grinds to a complete halt. Boards of firms like this need assurance that the technology systems are totally protected against potential operational disasters—computer bugs, power interruptions, hacking, and so on—and that costs remain under control.

Offensive IT places strategic issues either over, or on the same level as, reliability. Offensive IT projects tend to be ambitious and risky because they often involve substantial organizational change. An offensive stance is called for when a company needs to alter its technology strategy to compete more effectively or to raise the firm to a position of industry leadership. Because of the resources required to take an offensive position, financially and competitively strong companies usually have to be intensively involved in IT on all levels. Wal-Mart, for example, is replacing bar codes with radio frequency identification (RFID) technology, which effectively drives the supply chain directly from the supplier to the warehouse without the need for scanning by associates.

Firms can be either defensive or offensive in their strategic approach to IT—approaches we call "modes." Let's look at each mode in turn.

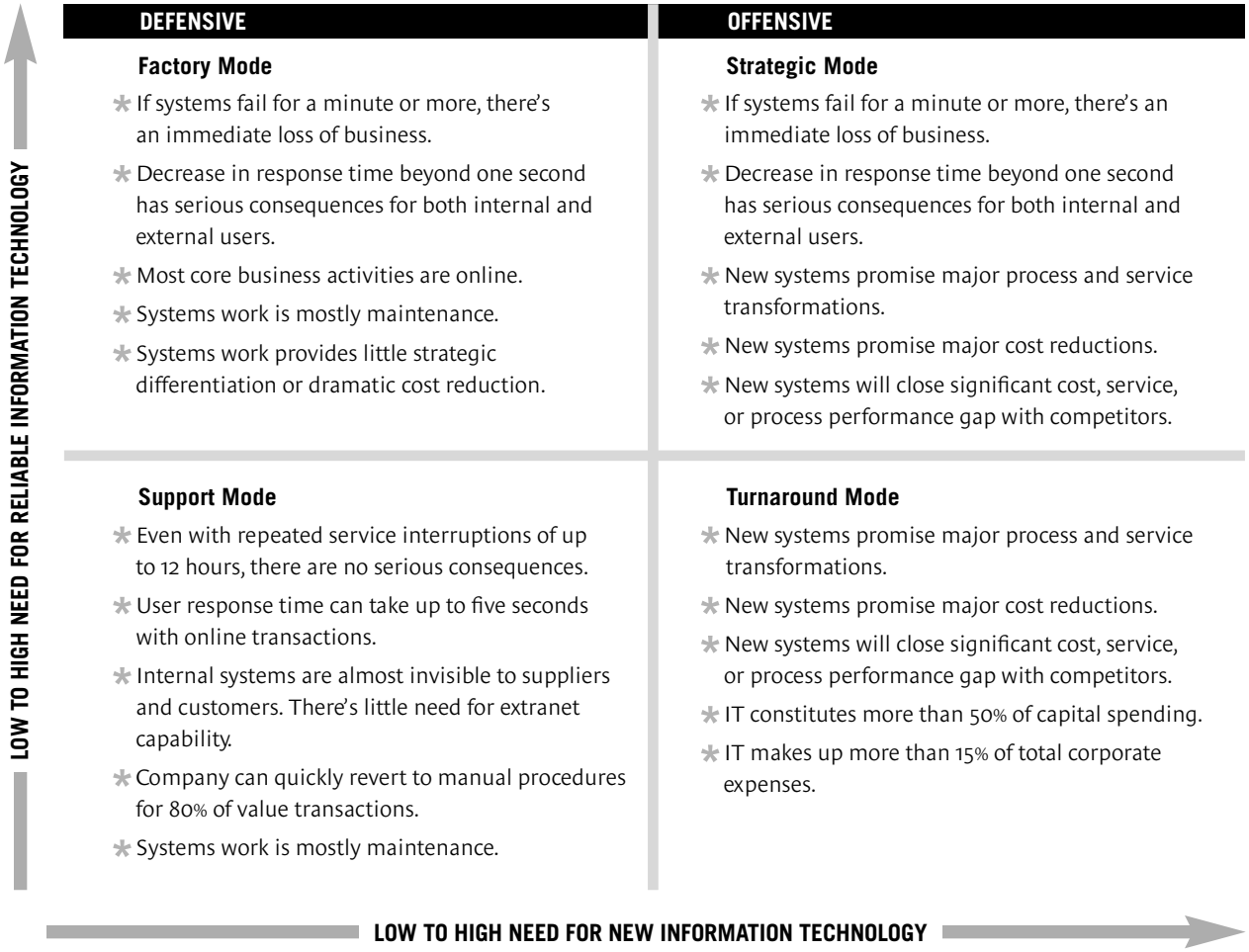
Richard Nolan (rnolan@hbs.edu) is an emeritus professor of business at Harvard Business School in Boston and a professor of management and organization at the University of Washington Business School in Seattle. **F. Warren McFarlan** (fmcfarlan@hbs.edu) is a Baker Foundation Professor and the Albert H. Gordon Professor of Business Administration emeritus at Harvard Business School.

Support Mode (Defensive). Firms in this mode have both a relatively low need for reliability and a low need for strategic IT; technology fundamentally exists to support employees' activities. The Spanish clothier Zara, which began as a small retail shop, is a good example; the company keeps strict control over its supply chain operations by designing, producing, and distributing its own clothing. Though IT is used in these areas, the company won't suffer terribly if a system goes down. (For more on Zara, see Kasra Ferdows, Michael A. Lewis, and Jose A.D. Machuca, "Rapid-Fire Fulfillment," HBR November 2004.) Core business systems are generally run on a batch cycle; most error correction and backup work is done manually. Customers and suppliers don't have access to internal systems. Companies in support mode can suffer repeated service interruptions of up to 12 hours without serious bottom-line consequences, and high-speed Internet response time isn't critical.

For such firms, the audit committee can review IT operations. The most critical questions for members to ask are: "Should we remain in support mode, or should we change our IT strategy to keep up with or surpass the competition?" and "Are we spending money wisely and not just chasing after new technol-

The IT Strategic Impact Grid

How a board goes about governing IT activities generally depends on a company's size, industry, and competitive landscape. Companies in support mode are least dependent on IT; those in factory mode are much more dependent on it but are relatively unambitious when it comes to strategic use. Firms in turnaround mode expect that new systems will change their business; those in strategic mode require dependable systems as well as emerging technologies to hold or advance their competitive positions.



ogy fads?" (In this mode, the spending mantra is, "Don't waste money." For a list of questions appropriate to each mode, see the exhibit "Asking the Tough Questions.")

Factory Mode (Defensive). Companies in this mode need highly reliable systems but don't really require state-of-the-art computing. They resemble manufacturing plants; if the conveyor belts fail, production stops. (Airlines and other businesses that depend on fast, secure, real-time data response fall into this group.) These companies are much more dependent on the smooth operation of their technology, since most of their core business systems are online. They suffer an immediate loss of business if systems fail even for a minute; a reversion to manual procedures is difficult, if not impossible. Factory-mode firms generally depend on their extranets to communicate with customers and suppliers. Typically, factory-mode organizations are not interested in being the first to implement a new technology, but their top management and boards need to be aware of leading-edge practice and monitor the competitive landscape for any change that would require a more aggressive use of IT.

Because business continuity in IT operations is critical for these firms, the board needs to make sure that disaster recovery and security procedures are in place. The audit committee for a large East Coast medical center, for example, recently authorized a full disaster recovery, security, and operational environment review simply to ensure that appropriate safeguards were there. The study was expensive but completely necessary because, in the event of a failure, patients' lives would be at risk. (In this mode, the spending mantra is, "Don't cut corners.")

Turnaround Mode (Offensive). Companies in the midst of strategic transformation frequently bet the farm on new technology. In this mode, technology typically accounts for more than 50% of capital expenditures and more than 15% of corporate costs. New sys-

Asking the Tough Questions

What board members need to know about IT depends on the company's strategic position. Firms in support and factory mode should have their audit committees, with the help of an IT expert, query management. Organizations in turnaround and strategic mode will want the assistance of a full-fledged IT committee in getting answers to their questions.

If your company is in **Support Mode,** ask the questions in set **A.**
If your company is in **Factory Mode,** ask the questions in sets **A** and **B.**
If your company is in **Turnaround Mode,** ask the questions in sets **A** and **C.**
If your company is in **Strategic Mode,** ask the questions in sets **A, B,** and **C.**

A

- Has the strategic importance of our IT changed?
- What are our current and potential competitors doing in the area of IT?
- Are we following best practices in asset management?
- Is the company getting adequate ROI from information resources?
- Do we have the appropriate IT infrastructure and applications to exploit the development of our intellectual assets?

B

- Has anything changed in disaster recovery and security that will affect our business's continuity planning?
- Do we have in place management practices that will prevent our hardware, software, and legacy applications from becoming obsolete?
- Do we have adequate protection against denial of service attacks and hackers?
- Are there fast-response processes in place in the event of an attack?
- Do we have management processes in place to ensure 24/7 service levels, including tested backup?
- Are we protected against possible intellectual-property-infringement lawsuits?
- Are there any possible IT-based surprises lurking out there?

C

- Are our strategic IT development plans proceeding as required?
- Is our applications portfolio sufficient to deal with a competitive threat or to meet a potential opportunity?
- Do we have processes in place that will enable us to discover and execute any strategic IT opportunities?
- Do we have processes in place to guard against IT risk?
- Do we regularly benchmark to maintain our competitive cost structure?

A lack of board oversight for IT activities is dangerous; it puts the firm at risk in the same way that failing to audit its books would.

tems promise major process and service improvements, cost reductions, and a competitive edge. At the same time, companies in this mode have a comparatively low need for reliability when it comes to existing business systems; like companies in support mode, they can withstand repeated service interruptions of up to 12 hours without serious consequences, and core business activities remain on a batch cycle. Once the new systems are installed, however, there is no possible reversion to manual systems because all procedures have been captured into databases.

Companies usually enter turnaround mode with a major IT project that requires a big reengineering effort, often accompanied by the decision to outsource or move a substantial portion of their operations offshore. Most firms don't spend a long time in turnaround mode; once the change is made, they move into either factory mode or strategic mode. American Airlines functioned in turnaround mode when it created the SABRE system; now it lives in factory mode. Similarly, the Canadian company St. Marys Cement operated in support mode until it began equipping its trucks with GPS devices, which pushed it into temporary turnaround mode.

Board oversight is critical for companies in turnaround mode; strategic IT plans must proceed on schedule and on budget, particularly when competitive advantage is at stake. (Here, the spending mantra is, "Don't screw it up.")

Strategic Mode (Offensive). For some companies, total innovation is the name of the game. New technology informs not only the way they approach the marketplace but also the way they carry out daily operations. Strategic-mode firms need as much reliability as factory-mode firms do, but they also aggressively pursue process and service opportunities, cost reductions, and competitive advantages. Like turnaround firms, their IT expenditures are large.

Not every firm wants or needs to be in this mode; some are forced into it by competitive pressures. Consider Boeing, a company that dominated the commercial-airline-manufacturing industry until Airbus took the lead. Now convinced that its future rests on the successful design, marketing, and delivery of a new commercial plane, Boeing has embarked on an ambitious technology project that it hopes will return the company to industry dominance. Its new 787 plane, due in 2008, will be equipped with a new lightweight carbon composite skin. Since carbon composite skin is a relatively new material to be used so extensively in a commercial airplane, a neural network will be embedded in the fuselage and wings to constantly monitor load factors and make adjustments as changing conditions warrant. The 787 will be manufactured and assembled through the world's largest project management system, which will simultaneously coordinate thousands of computers and automate an integrated supply chain comprising hundreds of global partners. Each supplier will send components via specially equipped 747s to Boeing's site in Everett, Washington, where the 787 will be assembled in a mere three days, ensuring low costs and fast delivery. The 787 is like a jigsaw puzzle whose pieces must fall into perfect alignment at once, making Boeing both operationally and strategically dependent on IT.

As is the case for firms in turnaround mode, board-level IT governance is critical in strategic mode. Organizations require a fully formed IT oversight committee with at least one IT expert as a member. (The mantra for strategic-mode companies is, "Spend what it takes, and monitor results like crazy.")

As we said at the outset, the specific action a company should take with respect to IT oversight depends on which mode it's in. Regardless of its business, it behooves any company to take an in-depth look at its current business through the IT lens. In doing so, a company gains a much firmer grasp of what it needs to be successful.

How to Conduct IT Oversight

Having identified which mode they currently inhabit, companies then need to decide what kind of IT expertise they need on the board. Firms that require a high level of reliability need to focus on managing IT risk. The job of these boards is to assure the completeness, quality, security, reliability, and maintenance of existing IT investments that support day-to-day business processes. Rarely will such companies want a separate IT committee. Instead, the audit committee must do double duty as the IT governance team and delve deeply into the quality of the company's IT systems.

On the other hand, companies that need to go beyond defensive mode require an indepen-

The IT strategy that works for a clothing retailer is not appropriate for a large airline; the strategy that works for eBay can't work for a cement company.

dent IT governance committee, rather than just having an IT expert serve on the audit committee. The IT governance committee's job is to keep the board apprised of what other organizations—particularly competitors—are doing with technology. Below, we outline the general duties of boards according to their modes.

Inventory the assets (all modes). A board needs to understand the overall architecture of its company's IT applications portfolio as well as its asset management strategy. The first step is to find out what kinds of hardware, software, and information the company owns so as to determine whether it's getting adequate return from its IT investments.

Physical IT assets—counted as computer hardware—are relatively easy to inventory; intangible assets are not. Despite the fact that intangible assets have largely been ignored by the accounting field, most companies are increasingly reliant on them. Companies have huge investments in applications software, ranging from customer and HR databases to integrated supply chains. The board must ensure that management knows what information resources are out there, what condition they are in, and what role they play in generating revenue. One rule of thumb in determining intangible assets is to first measure the hardware inventory—including all mainframes, servers, and PCs—and then multiply that by ten. This renders a rough notion of what the software inventory will be (including off-the-shelf and proprietary software). The next step is to assure that the IT organization sorts the wheat from the chaff by determining the number and location of aging and legacy programs, and then decide which should be upgraded or maintained.

The board will also want to ensure that its company has the right IT infrastructure and applications in place to develop intellectual assets such as customer feedback about products and services. It needs to know how well employees can use IT systems to analyze customer feedback and develop or improve products and services.

Assure security and reliability (factory and strategic modes). Ideally, boards of companies in factory and strategic modes should conduct regular reviews of their security and reliability measures so that any interruption of service doesn't send a company into a tailspin. Unfortunately, and all too often, oversight takes place following a crisis.

With the development of highly integrated IT networks within and outside the company, proper security has become paramount. An attack by a hacker or a virus can reduce profits by millions of dollars. An attack on Amazon, for example, would cost the company $600,000 an hour in revenue. If Cisco's systems were down for a day, the company would lose $70 million in revenues. Thus, the board needs to ensure that management is continually evaluating the company's networks for security breaches. (Some companies actually work with would-be hackers to test vulnerability to threats.)

A board will also want to make sure that service outages don't occur in the case of power failures or natural disasters. IT services are analogous to electrical power; an outage of days can trigger the demise of a company, particularly one in defensive mode. For this reason, backup systems must be continually tested to make sure that they actually work. IT also needs to ensure that service continues even while maintenance is under way, so proper detours and backups need to be in place. Many companies use diesel generators to keep backup systems running, but as the gigantic power outage that struck the East Coast of the U.S. in August 2003 demonstrated, the diesel can run out if the backup systems are in continuous use. In such cases, companies must take special steps. (Following the 2003 blackout, Delta Air Lines arranged for generator fuel to arrive by helicopter in the event of another shortage.)

Avoid surprises (factory, turnaround, and strategic modes). No board wants to be taken unawares, and the most frequent source of IT-related surprises is from lax or ineffective project management. The larger the IT project, the higher the risk. Consider what happened to candy maker Hershey's when an expansion of its brand new ERP system blew up in the company's face. By the time Halloween rolled around, the company still could not keep track of orders, revenues, and inventory. Best estimates are that this cost the company $151 million.

Even companies that are supposed to be technology experts can botch a project, as EDS proved when it lost $2 billion on a contract to build an intranet for the U.S. Navy. Because

EDS didn't fully understand the scope of the strategically important Navy initiative, the project suffered from unexpected delays and technical setbacks, costing EDS massive write-downs that ultimately drove its debt to junk bond status. To avoid such unwanted surprises, boards must ensure that appropriate project management systems are in place and that key decision points along the way are elevated to the appropriate level so that management can decide whether the project is still worth doing.

Companies can also be caught unawares if they don't have adequate service level agreements (SLAs) with vendors or clients, particularly when they choose to outsource their IT activities. A solid, well-thought-out SLA that makes explicit specific terms, deliverables, and responsibilities can help firms avoid serious project management problems. The agreement should guarantee that the needs of all the diverse groups within the company—such as marketing, sales, call center operations, and bad debt collection—are met under the terms of the agreement.

Additionally, legacy systems can present unwanted surprises because companies are so dependent on them, as the Y2K problem demonstrated. Rather than replace those systems, companies tend to build on top of them. And firms running batch-oriented systems often overlay them with new online user interfaces. This can create serious problems for accounting departments: A user of an online query system, for example, may believe that the answer he or she receives is up-to-the-minute; but if, in fact, data files are updated in batch mode, the information could be many hours out of date. Having to sort through such misinformation might require accounting departments to hire additional staff to ensure that financial reporting is done on time. To avoid such problems, the governance committee needs to decide whether it is more economical to maintain legacy hardware, software, and applications or to replace them. It's relatively easy for IT departments to determine when computer hardware needs upgrading. But when it comes to intangible assets such as legacy databases, the question of maintenance versus replacement becomes trickier; it's not uncommon to find maintenance taking up 90% of IT programming expenditures.

Watch out for legal problems (turnaround and strategic modes). Companies can be subject to legal problems if they don't tread carefully around the intellectual property issues relating to IT. The advent of the Linux operating system, for example, has been a boon to many companies; at the same time, making free use of associated patented intellectual property has exposed them to legal risks. Consider SCO's $3 billion lawsuit against IBM, in which SCO alleges that IBM illegally incorporated SCO's intellectual property to the code base of the Linux operating system. Cases like this have made it clear that organizations need to stay alert for possible problems and avoid the expensive distraction of an intellectual property dispute involving IT. The board needs to watch out for such risks and be ready to bring in appropriate legal counsel when necessary to keep the senior management team from being distracted.

Keep an eye out for fresh threats and opportunities (turnaround and strategic modes). It's a good idea for committee members to interrogate the CIO and line management about new products they may have seen or heard about at technology trade shows or industry conferences. It is also good practice to monitor firms in other industries that have a reputation for making effective use of leading-edge technology applications.

The committee must be on the lookout for technology-based competitive threats that could place a company in what we call "strategic jeopardy," which occurs when executive management is asleep at the switch vis-à-vis the competition. For example, the board can hire, or ask management to hire, a consulting company to gather intelligence, do benchmarking, and develop a scenario of possible threats from competitors, as well as outline opportunities. IT committees should also be sure that management has created a good customer feedback system that allows customers to offer opinions about competitors' products and services. In addition, it's important to monitor companies that may have the means and inclination to become competitors. Had supermarket chains been apprised of what Wal-Mart was up to with RFID, they might not have found themselves blindsided by the retail giant's aggressive supply-chain advances in the grocery business.

Finally, boards of firms in offensive modes must constantly scan for opportunities as technologies advance and the cost of computing

drops. Anything that has been performed manually, for example, presents an opportunity not only to automate but also to raise the bar for products or services. Otis Elevator, for instance, dramatically improved its product delivery cycle by intelligently using IT to replace a paper-based tracking and fulfillment system. Once a contract for an elevator, escalator, or walkway is signed, a program called eLogistics sends project information directly from the field via nearly 1,000 local area networks and 1,000 global wide-area networks to contract logistics centers. The result has been a huge drop in inventory and a fivefold improvement in delivery time.

Building the IT Governance Committee

How do you set up an IT governance committee? A company that decides it needs board-level IT oversight must do three things: select the appropriate members and the chairman, determine the group's relationship to the audit committee, and prepare the charter. The first two are especially important.

The IT expert's job is to challenge entrenched in-house thinking. He or she must be a skilled communicator who does not hide behind technology jargon or talk down to board members.

We recommend that the IT governance group be made up of independent directors, as is the case with audit and compensation committees. Chairmanship is also critical. For firms in support, factory, or turnaround modes, the chairperson need not be an IT expert but should certainly be a tough-minded, IT-savvy business executive—either a CEO or a top manager who has overseen the use of IT to gain strategic advantage in another organization.

In any case, at least one person on the committee should be an IT expert who should operate as a peer at the senior management and board level. The expert's job is to challenge entrenched in-house thinking. He or she should not think ill of technology-averse cultures and must be a skilled communicator who does not hide behind technology jargon or talk down to board members. The expert should help the committee avoid dwelling on the difficulties of the work and emphasize instead the opportunities. The focus should be on the big picture: Conversations about IT strategy are hard and can be discouraging if the committee gets dragged down in technical details. (In fact, when looking for someone who fits these criteria, boards may find that many talented CIOs and CTOs drop off the list of potential IT committee members.) The IT expert must have not only a solid grounding in the firm's overall business needs but also a holistic view of the organization and its systems architecture. This is particularly important if the firm chooses to outsource its functions and connect multiple vendors across a network. The expert must also thoroughly understand the underlying dynamics governing changes in technology and their potential to alter the business's economic outlook.

Generally speaking, the IT expert serves much the same function as the certified financial expert on an audit committee. A CIO or CTO with solid experience in the management of IT qualifies; for example, the IT oversight committee chairman for the Great Atlantic & Pacific Tea Company (A&P) was previously CEO of an extremely successful supermarket chain on the West Coast, where he achieved impressive business results through effective IT system implementation and management. As chair of the IT committee, he helps balance his company's short-term business needs with long-term IT investments.

Unfortunately, skilled, business-oriented technology strategists are in short supply. In the absence of such a person within a company, an IT consultant who can help sort out technology issues can fit the bill, as might a divisional CEO or COO who is actively managing IT. Alternatively, a manager who has served in an influential technology company such as Microsoft or Oracle can help a firm determine its place on the strategic impact grid, begin to embrace emerging technologies, and locate other experts who can serve on the committee.

Businesses in strategic mode should have an IT oversight committee chaired by an IT expert. In this mode, it's even more important to get the membership right. For example, the chairman of the IT committee for Novell—a company in strategic mode—founded a major IT-strategy-consulting company, sold it to one of the then Big Six accounting firms, and continued as a senior partner in that firm's IT consulting business. Two other members of Novell's IT committee previously served as CIOs in major *Fortune* 100 companies; they also serve on Novell's audit committee.

We recommend that the relationship of the IT governance committee to the audit committee be very close, because IT issues can affect economic and regulatory matters such as

An IT Governance Committee Calendar

To be successful, an IT oversight committee must ensure that its discussions with senior management are deep and ongoing. The committee can help management visualize IT's impact on the firm. We recommend that it develop a to-do calendar of the defensive, offensive, and administrative oversight tasks it needs to carry out over the year. Here's a sample calendar.

DEFENSIVE GOVERNANCE	Frequency
IT Projects/Architecture	
Receive update of strategic projects.	Quarterly
Receive update of technical architecture and critique it.	As Needed
Ensure update of applications architecture and critique it.	As Needed
Receive and review update of project investments.	Annual
IT Security	
Critique IT security practices.	Annual
Review and appraise IT disaster-recovery capabilities.	Annual
Review security-related audit findings.	As Needed
Review current developments in security practices, standards, and new security-related technology strategies.	Annual
Internal Controls	
Review IT internal control practices.	Annual
Review IT-related audit findings.	As Needed
Send reports to audit committee regarding IT systems and processes affecting internal controls.	Annual

OFFENSIVE GOVERNANCE	Frequency
Advisory Role	
Advise senior IT management team.	As Needed
Stay informed of, assess, and advise the company's senior IT management team about new technologies, applications, and systems that relate to or affect the company's IT strategy or programs.	As Needed
Receive update of IT strategy and critique it.	Annual
Review and critique business plan (annual and three-year).	Annual
Review internal IT assessment measurements and critique action plan.	Annual
Hold private session with CFO.	Quarterly
Strategic Technology Scanning	
Visit other companies to observe technology approaches and strategies.	Annual
Engage outside experts as required to provide third-party opinions about the company's technology strategy.	As Needed
Report to the board on matters within the scope of the committee, as well as on any special issues that merit the board's attention.	Quarterly
Perform other duties as appropriate to ensure that the company's IT programs effectively support the company's business objectives and strategies.	As Needed

ADMINISTRATIVE	Frequency
Review and assess the adequacy of the IT oversight charter and recommend proposed changes to the board.	As Needed
Evaluate IT oversight committee's effectiveness (self-assessment).	Annual
Approve minutes of prior meetings.	Quarterly
Present report to board regarding the IT oversight committee's activities.	Annual
Hold executive session with committee members.	As Needed
Approve IT committee meeting planner for the upcoming year, and approve mutual expectations with management.	Annual

Sarbanes-Oxley compliance. For this reason, it's a good idea to have one audit committee member serve on the IT oversight committee. The charter of the IT committee should explicitly describe its relationship to the audit group, as well as its organization, purpose, oversight responsibilities, and meeting schedule (see the exhibit "An IT Governance Committee Calendar").

• • •

Regardless of a company's position, top-level commitment is critical if the board is to engage in IT governance. Board members and senior managers must identify and carefully gauge their current positions on the IT impact grid and decide whether setting up an IT oversight committee is necessary, given the company's current situation. If the need is not clearly understood, or if general buy-in for establishing such a committee—which necessarily includes an IT expert among its members—doesn't exist, then the company shouldn't do it. Any effort to do so will be a waste of time, and failure will sour the chances of establishing such a committee later.

That said, it's clear that as more and more companies in support and factory modes change tactics, and as other firms choose to adopt new technologies to stay ahead of the game, board-level technology governance will become increasingly important. This is good news, for when top managers understand the degree to which they must be accountable for technology, for project expenditures, and for monitoring return on investment from IT, they will do a better job of ensuring that critical systems function as promised. One thing is certain: Given the dizzying pace of change in the world of technology, and the changes IT can force upon a business, there is no such thing as too much accountability.

Reprint R0510F
To order, see the next page
or call 800-988-0886 or 617-783-7500
or go to www.hbr.org

Harvard Business Review OnPoint

Harvard Business Review OnPoint articles enhance the full-text article with a summary of its key points and a selection of its company examples to help you quickly absorb and apply the concepts. *Harvard Business Review* OnPoint collections include three OnPoint articles and an overview comparing the various perspectives on a specific topic.

Further Reading

The *Harvard Business Review* Paperback Series

Here are the landmark ideas—both contemporary and classic—that have established *Harvard Business Review* as required reading for businesspeople around the globe. Each paperback includes eight of the leading articles on a particular business topic. The series includes over thirty titles, including the following best-sellers:

Harvard Business Review on Brand Management
Product no. 1445

Harvard Business Review on Change
Product no. 8842

Harvard Business Review on Leadership
Product no. 8834

Harvard Business Review on Managing People
Product no. 9075

Harvard Business Review on Measuring Corporate Performance
Product no. 8826

For a complete list of the *Harvard Business Review* paperback series, go to www.hbr.org.

Harvard Business Review

To Order

For reprints, *Harvard Business Review* OnPoint orders, and subscriptions to *Harvard Business Review:*
Call 800-988-0886 or 617-783-7500.
Go to www.hbr.org

For customized and quantity orders of reprints and *Harvard Business Review* OnPoint products:
Call Rich Gravelin at 617-783-7626,
or e-mail him at rgravelin@hbsp.harvard.edu