PwC Directors and IT- What Works Best

An Alternate View

by

Janice Giannini

I recently had the opportunity to read PwC's "Directors and IT—What Works Best." The report is a comprehensive discussion of a process for helping directors get their arms around effective IT oversight. The framework presents an approach for understanding and governance of IT that aligns with current thinking around company strategy and IT capabilities. The idea is that one needs to understand IT, its ramifications, and its potential before aligning it with where the company is going. I describe this approach as a bottom-up analysis: start with what you know and where you are to determine how you want to align and monitor.

Some of the salient features of the report are:

- There is an IT confidence gap for many directors of public company boards today. The gap is driven by insufficient knowledge of IT and technology, as well as lack of process for understanding and evaluating the environment.

- Part 1 provides a framework of six steps to aid directors' understanding and ability to oversee the company's efforts: Assessment, Approach, Prioritization, Strategy, Risk, and Monitoring. There is also a checklist of questions to facilitate the conversation in these areas.

- Part 2 contains a discussion of several timely topics for boards today, including data security, mobile computing, data privacy, social media, cloud services, and streamlining business processes using digital means.

Implementing the steps of the framework in the order presented in the report will likely lead to the following positive results:

- Clear current-state definition and understanding of IT capabilities
- Alignment between management and the board on an IT oversight approach
- Prioritization of IT efforts
- Opportunity to build IT efforts into the company strategy
- Opportunity to build IT risk into overall company risk management activity
- A process for monitoring progress over time

There may also be several potential unintended consequences of this approach:

- Prioritization of the IT budget that is not directly linked to the business area and company growth profile
- Internal conflicts between business areas and functional organizations
- Absence of a total cost-benefit for investment in maintenance capabilities/risk and growth capabilities/risk
- Introduction of greater risk if alignment between business growth and IT strategies is less than optimal
- A belief that IT strategy may be separate from overall company strategy

I offer an alternate framework, one that preserves the strength of the individual steps while addressing the unintended consequences above.

Instead of executing the steps in this order:	Execute them in this order:
• Assessment	Strategy
• Approach	Prioritization
• Prioritization	Risk
• Strategy	Assessment
• Risk	Approach
• Monitoring	Monitoring

The company strategy drives the line of business (LOB) strategy, which drives product/service strategy. The strategy for each LOB must include all necessary and sufficient elements to produce the desired outcome, i.e., revenue and profit.

It is important to note the difference between *strategies* and how one chooses to structure the company to accomplish work. A company may choose to create a structure to accomplish work that assigns all of the technology or IT resources to one organization and call it the CIO's organization. That does not mean the IT function has a strategy independent and distinct from the company. In this regard, IT is no different from marketing, sales, or any other function.

A company develops a three- to five-year strategy. To achieve those strategic goals, the LOBs develop strategies and implementation plans for products and services, along with necessary cost structure and capabilities. An integrated, holistic, cross-functional team and plan are needed to make everything happen. IT is *part* of that team. It's a significant part, but it's not a separate entity.

This alternate lens acknowledges that the company plan requires cross-functional inputs and collaboration to get a job accomplished and that all parts must be consistent from the outset. That is very different from a belief that IT strategy is separate and must be aligned at some point during the process.

The Directors' role is to ensure that the strategy, technology and the plans are consistent across the company so the operational growth is executable and the appropriate technology is there to support that growth. In addition, directors need to be aware of the potential for disruptive technologies/ innovation to balance the short term and the long term when evaluating business risk. This integrated holistic view better equips directors to ask the right questions to understand the" tightness of the integration" and the quality of the risk. This insight is a critical element of guiding the balance of risk and investment.

Don't you get to the same place, regardless of the order of the steps in the framework?

Actually, no. If the entire executive team collaborates on the strategy, there is consistency from the start, and the framework will play out differently.

With a top-down approach, the executive team and the board have a much better chance of staying in alignment from strategy to LOB to functional execution, and they can do this across all functions more easily. If the board's responsibility is ensuring that the strategy, risk, and execution are appropriate, then having the big picture allows it to put the puzzle together more easily. It also facilitates replacing a puzzle piece when things get bent or broken.

Similarly, a top-down approach creates better results for the company at the operational level because of greater collaboration and respect across functions.

Rationale

Step 1 is strategy. It is difficult to have a meaningful conversation around technology or IT without a strong understanding of the overall company strategy, the LOB strategy, and the needs of the product or service team. Starting anywhere else leads to incomplete and potentially misleading conclusions. The initiatives are not *IT* initiatives; they are company initiatives driven by a business need. If they are not driven by a business need, then why are they being done?

Top-down thinking allows clarity of thought around company initiatives. For example, an ERP implementation involves the entire company and requires a committed, integrated, cross-functional team to facilitate the many changes that will be needed across the company to be successful. In the absence of that, the implementation will fail because it was not a collaborative, cross-functional effort. If the implementation is viewed as an IT-only initiative, when it fails, one response might be that IT didn't deliver. What really happened is that the company set itself up for failure.

Step 2 is prioritization. Once you understand the company strategy, the LOB strategy, and the product and service strategy, then you are in a position to understand what items need board-level insight. If you prioritize before the integrated strategic understanding, small but critical elements may get lost in the shuffle—or you may focus on the wrong things.

Once the company determines what it will invest and what it will not invest, the board can determine the right level of oversight. If the company chooses to say to an LOB, "We are not investing, do the best you can," board oversight may not be needed. The board may also have a responsibility to understand the rationale for not investing, since non-investment may increase risk. The board must be in alignment with the risk appetite the company is assuming.

Step 3 is risk. The risk assessment follows directly from strategic choices and prioritization. Risk assessment and mitigation requires addressing the risk for initiatives undertaken and those not undertaken. By looking at the company top down, you don't need to remember to bake IT into the discussion; it's already in the discussion.

Step 4 is IT assessment. An understanding of the overall strategy, priority, and risk creates the context in which to conduct an IT assessment. The objective is to go beyond understanding what capabilities exist and answer to such questions as: "Is what we have good enough?" and "Where are the opportunities and weak links?" The analogy I use is this: I have $5,000, is that good, bad, or neither? If I live in the US, it may be one month’s living cost. If I live in sub-Saharan Africa, it likely represents food security and, potentially, education security for my children. The context matters. Some IT and technology activities will be LOB specific; others will cut across the company. It is imperative that the senior executives and the board understand the difference between the two and own the consequences.

Step 5 is approach. Once the scope of the job is clear, it is time to determine the best approach for the board to exercise oversight.

Step 6 is monitoring. As with all activities, initiatives, or special events, continuous process improvement and measurement are critical.

By adjusting the order of the framework steps, the board can use a single process for oversight, eliminating the need for an IT-only process. The content of the discussion will be different and IT related, but the process will be the same. This takes some of the mystery out of IT and helps increase board confidence.

Technology experts belong on boards

The body of the PwC report contains a section related to who on the board is accountable for IT oversight. Several theories were advanced, including the audit committee, a risk committee, and the whole board. Because technology either strengthens a company’s foundation or weakens it, a separate technology committee will be needed in many companies. This option may be unpopular because it requires additional resources, but the consequences of insufficient oversight are dire.

The report states that only 30% of current directors feel it’s important to have technology experts on the board. Given the importance of technology to businesses today, I strongly encourage directors to reconsider.

I also challenge the assumption in the report that getting someone who understands technology on the board means giving up someone with a broader business perspective. Today, it’s quite possible to have both. An executive with P&L, operations, product development, and CIO experience has much to bring to the table.

Many boards use external consultants in lieu of having such expertise on the board. I believe this is a good solution in many cases, as they often have deep knowledge. However, it’s important to pair that person with a director who understands technology *and* the company and can clearly articulate the business implications.

At the end of Part 2, this question is asked: Is someone in the company thinking creatively about how to better leverage IT to get things done? I believe that as long as the answer to this is a person or persons (versus the leadership at all levels of the company, from the janitor to the CEO), there is a disconnect. With this disconnect comes an invitation for your competitors.

Understanding this at the 50,000-foot level for your company, with the attendant opportunities and their risk profiles, as well as the overall risk appetite of the company, is critical for all executives and directors. Ask yourself what you need to understand this. If you are not getting it, ask what needs to happen for you to obtain the information you need in a digestible manner. Those are critical questions that apply to the company as a whole, the LOBs, and every functional organization.

Summary

The PwC report presents a Framework that clearly addresses the critical elements of IT Governance.

As directors are guiding the company and balancing overall financials, risk, investment and growth curves, having access to an integrated top down assessment of the link among strategy, execution and technology is critical. In addition, with the advent of disruptive technologies/ innovations rapidly escalating, this top down approach further assists directors in their understanding of technology driven opportunities and the intended and unintended consequences of investment choices and risks.