

The Risk Intelligent
technology company
Managing risk to capture value



Contents

2	Preface
4	Managing risk to capture value
5	Risk redefined
6	Where do I begin?
8	What, me worry?
10	Capturing value
11	Contacts

Managing risk to capture value

A leading CEO once quipped that technology companies face only two risks: “Either you can’t build it or you can’t sell it.”

The statement generated a hearty laugh at the time, and, admittedly, there’s a certain appeal to the notion that risk can be distilled into such a tidy formula. Nonetheless, this pop analysis of the nature of risk won’t help you much if you’re a technology executive looking to preserve and create shareholder value. Where, for example, does fraud risk fit into the picture? Or regulatory, reputational, intellectual property, and environmental risk?

Consider the recent economic turmoil: Were you caught by surprise? Has your company been negatively impacted? Did other risks arise that you weren’t expecting? For most technology companies, the answer to those questions is a dispiriting “yes.”

The reality is that risk — and intelligent risk management — can’t be reduced to a glib sound bite. The topic is more nuanced, and your approach must be tailored to match.



Here’s another common misconception: *Risk management inhibits innovation.*

Not only is that assertion false, but the exact opposite is true. Nothing spurs creativity, encourages innovation, and enhances the pursuit of new ideas like a clear-eyed view of your opportunities and a frank assessment of the obstacles that might prevent you from capitalizing on them.

This is not to suggest that every idea will be a winner and every product a blockbuster. Failure can still rear its head no matter how effective the risk management program. However, in a Risk Intelligent environment, failures don’t bring down the company — or even profoundly impede its overall progress — because mechanisms are in place to provide early warning of things gone awry, and contingency plans stand ready to deal with adverse outcomes as they arise.

While many successful companies avoid risk, great companies embrace risk — but only after assessment, deliberation, understanding, and planning. This methodical, *Risk Intelligent* approach elevates the entire profile of success and failure, raising the peaks and filling in the valleys. As a result, the linkage between taking calculated risks and earning significant rewards becomes clearer, with plans in place to minimize the one while maximizing the other.

“While many successful companies avoid risk, great companies embrace risk ...”



Risk redefined

A prerequisite to describing Risk Intelligence is a clear definition of risk:

Risk is the potential for loss or harm — or the diminished opportunity for gain — that can adversely affect the achievement of an organization's objectives.

Note that this definition does not focus solely on the traditional realm of risk management — the protection of existing assets — but also encompasses risk-taking for reward. That is, organizations should devote commensurate resources to the risks associated with research and development, product rollouts, intellectual property, market expansion, mergers and acquisitions, strategic partnerships, and other growth and profit-enhancing activities. These are areas that propel success, and the risks associated with these activities can make a difference, not just between success and failure, but, perhaps more appropriately for most companies, between success and mediocrity.

Avoiding the flatline

The trend is so predictable it's almost uncanny: The trajectory of most technology start-ups will plateau at a certain stage. For some, the stall happens at \$1 billion in revenues. For others, it occurs 24 to 36 months along. But regardless of when it hits, the outcome can be disruptive: executive turnover, cold-footed investors, underwater options, and demoralized employees are just a few of the fallout.

But stunted growth is not inevitable — intelligent risk management can help keep your fortunes rising. Unfortunately, risk management is rarely a high priority at rapidly growing technology companies. "Vision" is king, and all available resources are devoted to attaining it. So perhaps the first thing that needs to change is the mindset. Don't abandon the vision — that's what energizes your people, spurs recruitment, and propels the organization forward. Instead, tweak the perspective. Bring into view those risks that could prevent you from meeting your aspirations around blockbuster products, marketplace dominance, and household name recognition.

Growth is the goal for any company, and for technology companies, growth is a strategic imperative. However, with rapid growth comes an evolving set of risks. A threat that might severely impede a technology company — such as the unexpected pullout of an important strategic partner — will dissipate over time as products are released and consistent revenue streams established. Yet the disappearance of one risk will often be accompanied by the appearance of another. For example, risk issues around the supply chain, innovation, and competition, among others, will arise as the company matures, while issues around new product development and customer acquisition might abate. As your organization changes, your perspectives on risk governance and processes must evolve as well.

In a Risk Intelligent environment, managers are continually looking ahead, peering into the future. This allows organizations to ready themselves for the next stage of growth, to anticipate impediments, and to avoid the flatlining that defines the trajectory of so many technology companies.



Characteristics of Risk Intelligence

Risk Intelligent Enterprises™ are companies that have attained an advanced state of risk management. Many characteristics define such companies. A Risk Intelligent Enterprise:

Develops Full-Spectrum Vision: Effectively assesses and manages risk across divisions, departments, companies, and geographies.

Bridges Silos: Acknowledges the need for risk specialization — deep knowledge of specific risks and responses — but constructs bridges between risk "silos."

Speaks a Common Language: Develops common risk terminology, so that everyone speaks the same language; and adopts common metrics, so that everyone measures risk in a comparable manner.

Assesses Impact: Realizes that, with a nearly infinite number of risks, planning for them all is impractical, if not impossible. Focuses on the finite impacts that could result from multiple threats.

Weighs Vulnerability: Augments the conventional risk management emphasis on probability by placing significant weight on vulnerability, since risk at the extreme is often the deadliest.

Considers Risk Interaction: Adopts an approach that does not solely consider single risk events, but also takes into account risk scenarios and the interaction of multiple risks.

Allocates Resources Appropriately: Conducts a comprehensive risk assessment and then prioritizes and focuses efforts on the areas of greatest risk.

Cultivates Risk Consciousness: Considers risk management an organization-wide responsibility, part of the everyday operations of the company and the routine duties of its people.

Pursues Risk Taking for Reward: Seeks not only value protection, but also pursues risk taking as a means to value creation.

Where do I begin?



Whether your intent is to establish a new or to enhance an existing risk management program, the prospect can seem daunting. Concerns about resource availability, internal competencies, and distraction from primary corporate objectives may arise. A few observations may ease these worries:

- 1) Your company is probably already engaged in more risk management than you realize. Your finance group is addressing reporting and regulatory risk. Your IT people are managing technology risk. Legal counsel is at work on IP risk. As such, your tasks may involve more coordination and harmonization, rather than starting from scratch.
- 2) You already have a wealth of risk and control expertise just waiting to be tapped within your organization — your internal audit group. Call in your chief audit executive (or equivalent) to discuss your internal capabilities.
- 3) A Risk Intelligence program can and should be staged rather than implemented wholesale. A phased-in approach allows you to move forward in a measured, rational manner with each element initiated, integrated, and assessed on an ongoing basis. This method has the additional benefit of putting fewer resource demands on your people and systems.
- 4) As noted previously, a properly implemented Risk Intelligence program would not distract from your primary corporate objectives, but rather would aid the attainment of those objectives as risks to corporate strategy and value creation are systematically identified, monitored, and mitigated.
- 5) Review your strategic assets (not just your physical assets), such as people, intellectual property, partners, etc., and ask yourself if your company is maximizing its value creation from them.

Whether your company is starting at the ground floor of risk management, or on a higher elevation, certain actions and activities should be on your risk agenda, including the following:

Raise risk awareness: Communicate the importance of effective risk management. These messages can be delivered in a variety of ways, such as meetings, newsletters, emails, and posters. In fact, the more varied the mode and frequent the delivery, the better likelihood of integrating the message.

Evaluate your risk framework: Effective risk management doesn't occur by happenstance or develop in an ad hoc manner. Rather, a structure is required to help you determine which business opportunities are worthy of pursuit and which hazards should be mitigated. A risk framework — such as COSO ERM, Turnbull, or ISO — provides that structure.

Speak the same language: Risk management often occurs in “silos” where specialists develop their own way of thinking, talking about, and measuring risk. But risks don't respect such artificial boundaries, and, in fact, have a tendency to combine and cascade in unexpected ways. To combat this, risk terminology and metrics should be harmonized and standardized across the organization.

Get on board: Boards and committees are often at a loss when it comes to their role in risk management. They are uncertain about roles and delineation of responsibility. They wonder about appropriate levels of oversight and how “hands-on” they should be. The answers are not simple, and they will vary from company to company, but just asking the questions in a formal setting will start an important dialogue.¹

¹ See *The Risk Intelligent Board: Viewing the World Through Risk-Colored Glasses* at www.deloitte.com/us/RiskIntelligence.

Peer outside your walls: Deploy a tool such as The Risk Intelligence Map™² to help identify the most important risks (and downstream impacts) that need to be managed.

Look at the upside: Conduct a scenario planning exercise to integrate upside risk management into your thinking. What are the threats that could prevent your company from attaining its growth and profitability objectives? How will you monitor and mitigate these threats? What events will trigger your action plan?

Take charge: Everyone is responsible for effective risk management, but the executive branch assumes the most prominent role — and possibly the most difficult. You need to view both the big picture and small details; offer the carrot and wield the stick; be intimately involved yet delegate freely; pull along the board, functions, and business units; inspire and be inspired.



Excerpted section from The Risk Intelligence Map for the Technology Sector. In its entirety, the map is a wall poster that depicts risks across the enterprise. For more information, and to obtain your own copy of The Risk Intelligence Map for the Technology Sector, contact your local Deloitte practitioner.

Foundational Principles of a Risk Intelligence Program

In a Risk Intelligent Enterprise™...

... a common definition of risk, which addresses both value preservation and value creation, is used consistently throughout the organization.

... a common risk framework supported by appropriate standards is used throughout the organization to manage risks.

... key roles, responsibilities, and authority relating to risk management are clearly defined and delineated within the organization.

... a common risk management infrastructure is used to support the business units and functions in the performance of their risk responsibilities.

... governing bodies (e.g., Boards, Audit Committees, etc.) have appropriate transparency and visibility into the organization's risk management practices to discharge their responsibilities.

... executive management is charged with designing, implementing, and maintaining an effective risk program.

... business units (departments, agencies, etc.) are responsible for the performance of their business and the management of risks they take within the risk framework established by executive management.

... certain functions (e.g., finance, legal, tax, IT, HR, etc.) have a pervasive impact on the business

and not only provide support to the business units as it relates to the organization's risk program, but also enhance and enable success when strategically aligned and considered as essential elements of the program.

... other functions (e.g., internal audit, risk management, compliance, etc.) provide objective assurance as well as monitor and report on the effectiveness of an organization's risk program to governing bodies and executive management.

For an elaboration on these principles, see *Putting Risk in the Comfort Zone: Nine Principles for Building the Risk Intelligent Enterprise* at www.deloitte.com/us/RiskIntelligence.

² Contact your Deloitte practitioner for information on The Risk Intelligence Map tool, or email rimap@deloitte.com.

What, me worry?

The technology industry is dynamic and fluid — and unforgiving. Today's hot products are tomorrow's landfill. Today's rising stars are tomorrow's one-hit wonders. Within this constant flux lurk many threats, of course, but also plentiful opportunities. Here are some of particular interest and concern to technology executives, along with some suggested Risk Intelligent responses.

Innovation: More so than any other industry, innovation fuels the tech sector. But the challenges are immense: Your competitors reverse-engineer your latest product before it even emerges from beta. Your industry opponents plan three product cycles ahead. Rival R&D labs churn out patents by the dozens.

In such an environment, speed to market becomes a critical concern, perhaps even more important than IP protection. Would your company be better served by focusing on birthing new ideas rather than defending old ones? Are there steps you can take to shorten the development timeline to stay a step ahead?

Risk Intelligent steps for fostering innovation

- 1) **Step up your competitive intelligence.** Determine what products your rivals have in the pipeline and how this will affect the life cycles of your products.
- 2) **Reach out and pull in your customers.** What will make them more productive, make their lives easier? Don't assume that more features and capabilities are desired; simplicity can be an equally strong driver. Ask them.
- 3) **Analyze your IP practices.** Just as an occupational bias makes most surgeons recommend the knife, most lawyers will advise for strong patent protection. Conduct an independent evaluation to determine if your resources could be better spent elsewhere.
- 4) **Scrutinize your supply chain.** How many days and weeks are you losing to supply chain inefficiencies, or could you lose due to supply chain vulnerabilities?
- 5) **Reward innovation.** The road to successful product development can be long, with many dead ends and detours along the way. As such, compensation and recognition should be focused on the steps rather than the final result. To foster innovation, reward behaviors, actions, and ability.



Mergers & Acquisitions: In the technology industry, as the saying goes, you are either the dinner or the diner. With the compelling need to fill in gaps in service or product offerings, there is simply no time to grow organically. Instead, M&A has become a core strategy for technology companies.

Yet M&A brings its own set of risks to the table. Companies must consider cultural and technological integration issues; be careful not to cannibalize their own distribution channels or customers; be wary about inheriting other companies' problems; and be careful about falling into a defensive M&A strategy.

Risk Intelligent steps for successful M&A

- 1) **Don't neglect post-merger integration planning and execution.** Many M&As fail due to a poorly planned (or unplanned) post-merger integration. Devote as many resources to integration activities after the deal is closed as you did in your pre-merger due diligence. Don't forget to align your legal entity structure and tax strategies.
- 2) **Analyze buy versus build.** Despite the trend toward M&A, buying what you need is not necessarily suitable for every situation. Carefully investigate the risks and opportunities of internal growth vs. acquisition or merger.
- 3) **Enhance your M&A radar.** With deals constantly springing up and falling through, you need a near-continuous monitoring mechanism.
- 4) **Be prepared to be acquired.** In many cases, shareholder value is enhanced by being acquired. An effective risk management program removes much of the unknown risk for buyers and increases the value of the company.
- 5) **Sustain the momentum.** Don't let enthusiasm for the deal dissipate post merger. Measure and reward against the results the merger was intended to attain. For example, if the combined IT departments were expected to generate 20 percent savings, build that goal into the CIO's performance evaluations and compensation package.



Third-party reliance/supply chain: Overdependence on a single supplier is a well-known business risk, and most companies have contingency plans in place to deal with disruptions and even the outright failure of a major partner. But have you attained an optimal balance between diversity of suppliers and economies of scale? Getting it right can have a significant impact on the bottom line. If you consolidate to fewer suppliers, you'll need to supplement that move with better risk management.

Increased reliance on third parties also creates a transparency dilemma. How do you manage the risk of information exposure? There are tradeoffs between the transparency that is required for a productive business relationship and the risk of giving away competitive information that could disadvantage your company.

Security and privacy issues also frequently arise in third-party relationships. A spider's web of state, federal, and international privacy laws and regulations can snag even otherwise risk-savvy organizations. Sharing of customer information can prove particularly vexing, as the U.S. Federal Trade Commission will hold companies accountable for the privacy policies stated on their websites, in print, and elsewhere. For example, if your company has collected customer information online, shared it with a vendor or partner, and then lost control of it, the negative repercussions — legal, monetary, and reputational — could be significant.

Risk Intelligent steps for effective supply chain management

- 1) **Understand that your partner's risk is your risk.**
Reliance on third parties can increase your profit potential but also elevate your risk profile. A relationship based on "trust but verify" is essential.³ Relationships are enhanced when any doubt is removed.
- 2) **Create a problem resolution process.** Disagreements happen. They are more readily rectified if you have a process in place for dealing with them. Use risk management to improve the relationship.
- 3) **Frankly assess.** Don't be satisfied with the status quo. Periodically ask your key people: What did we expect to get out of this relationship? What are we actually getting?⁴
- 4) **Understand the profit drivers in your supply chain.**
Then consider where, why, when, and how they are taxed. Are you paying more, or less, than you should?

³ See *Using Contract Risk & Compliance to Manage Risk and Enhance Value* at www.deloitte.com/us/crc.

⁴ See *The Risk Intelligent Approach to Outsourcing and Offshoring* at www.deloitte.com/us/RiskIntelligence.

Access to, and efficient use of, capital: In the technology industry, capital requirements continually shift as companies move through their life cycles. But regardless of the stage of development, for most tech executives, it probably feels like the acts of pursuing capital, managing cash flows, courting investors, structuring debt, and other capital-related activities consume an inordinate amount of time.

The key to channeling the ebbs and flows, minimizing the cost of capital, and eliminating the time sink lies in a Risk Intelligent analysis and planning exercise that maps development stages and major milestones against capital needs. Determining exactly when you will require an infusion will reduce treasury risk and help you balance the downside of sitting on too much cash with the risk of coming up short. A scenario-planning activity that envisions various growth trajectories is the first step toward a comprehensive treasury management plan. Always being ready to maximize a sudden opportunity is paramount.

Risk Intelligent steps for efficient access to, and use of, capital

- 1) **Analyze based on stages of growth.** The capital requirements of your company will evolve as you grow. Project what your business might look like over the next 2, 5, and 10 years (or until your anticipated liquidity event). Then identify what impact that growth will have on your need and ability to raise capital.
- 2) **Don't neglect the human component of capital.**
As part of your scenario planning, determine what your talent needs will be (in finance and elsewhere), then develop plans for recruiting, training, and promotion to meet those needs.
- 3) **Be tax savvy.** Funding isn't only about the "when," but also about the "where." Structure your capital to take advantage of the most favorable tax outcomes. Where are the funds coming from? How will you get the money where it needs to be? Global companies require global tax strategies, which, in turn, require additional risk management.

Capturing value

Mention the words “risk management” to many top technology executives and chances are their eyes will glaze over. In their view, risk management is the domain of middle managers. They believe that the C-suite is paid top dollar to create shareholder value, not to worry about inventory losses or plant safety.

Yet risk doesn’t impact only existing assets. Threats to the attainment of your business objectives are just as real and can have profound consequences in the pursuit of success. Every business strategy, goal, milestone, and aspiration has associated risks that can make the difference between success, mediocrity, and failure. Thus, it is proper to assert that risk management is — or should be — a C-suite concern.

For most technology companies, risk management is about managing the risks you know. Risk Intelligence, on the other hand, is about managing risk when “you don’t know what you don’t know.”

Intelligent risk taking can provide a competitive edge, and with the proper risk framework in place, risk taking can flourish and pay dividends. Innovation and creativity are enhanced, because people know the bets they are placing have been vetted, that their decisions are supported, and that a safety net is in place.

The opening paragraph of this document criticized as overly simplistic the notion that only two risks face technology companies. In its stead, here’s another phrase, equally brief, but considerably more apt:

To capture value, manage risk.



Contacts

Mark Jensen

U.S. Audit and Enterprise Risk Services
Technology Leader
Deloitte & Touche LLP
+1 408 704 4790
mejensen@deloitte.com

Eric L. Openshaw

Vice Chairman and U.S. Technology Leader
Deloitte LLP
+1 714 913 1370
eopenshaw@deloitte.com

Henry Ristuccia

Partner
Governance, Risk & Regulatory Services
Practice Leader
Deloitte & Touche LLP
+1 212 436 4244
hristuccia@deloitte.com

Philip L. Asmundson

Vice Chairman and U.S. Technology,
Media & Telecommunications Leader
Deloitte LLP
+1 203 856 9295
pasmundson@deloitte.com

A. Scott Baret

Partner
Deloitte & Touche LLP
+1 212 436 5456
sbaret@deloitte.com

Rita R. Benassi

Partner
Deloitte Tax LLP
+1 203 761 3740
rbenassi@deloitte.com

Donna Epps

Partner
Deloitte Financial Advisory Services LLP
+1 214 840 7363
depps@deloitte.com

Michael Fuchs

Principal
Deloitte Consulting LLP
+1 212 618 4370
mfuchs@deloitte.com

Garrett Herbert

Partner
Deloitte & Touche LLP
+1 408 704 2975
gaherbert@deloitte.com

H. Schaffer Hilton

National Managing Director
Technology, Media & Telecommunications
Deloitte Consulting LLP
+1 404 631 3226
shilton@deloitte.com

Eddie Leschiutta

Managing Partner
Enterprise Risk Services
Deloitte Canada
+1 416 601 5841
eleschiutta@deloitte.ca

Sandy Pundmann

Partner
Deloitte & Touche LLP
+1 312 486 3790
spundmann@deloitte.com

Alvin L. Royse

National Tax Managing Partner
Technology, Media & Telecommunications
Deloitte Tax LLP
+1 415 783 4794
aroyse@deloitte.com

Orlando Setola

Principal
Deloitte Financial Advisory Services LLP
+1 212 436 5607
osetola@deloitte.com

This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering business, financial, investment, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.