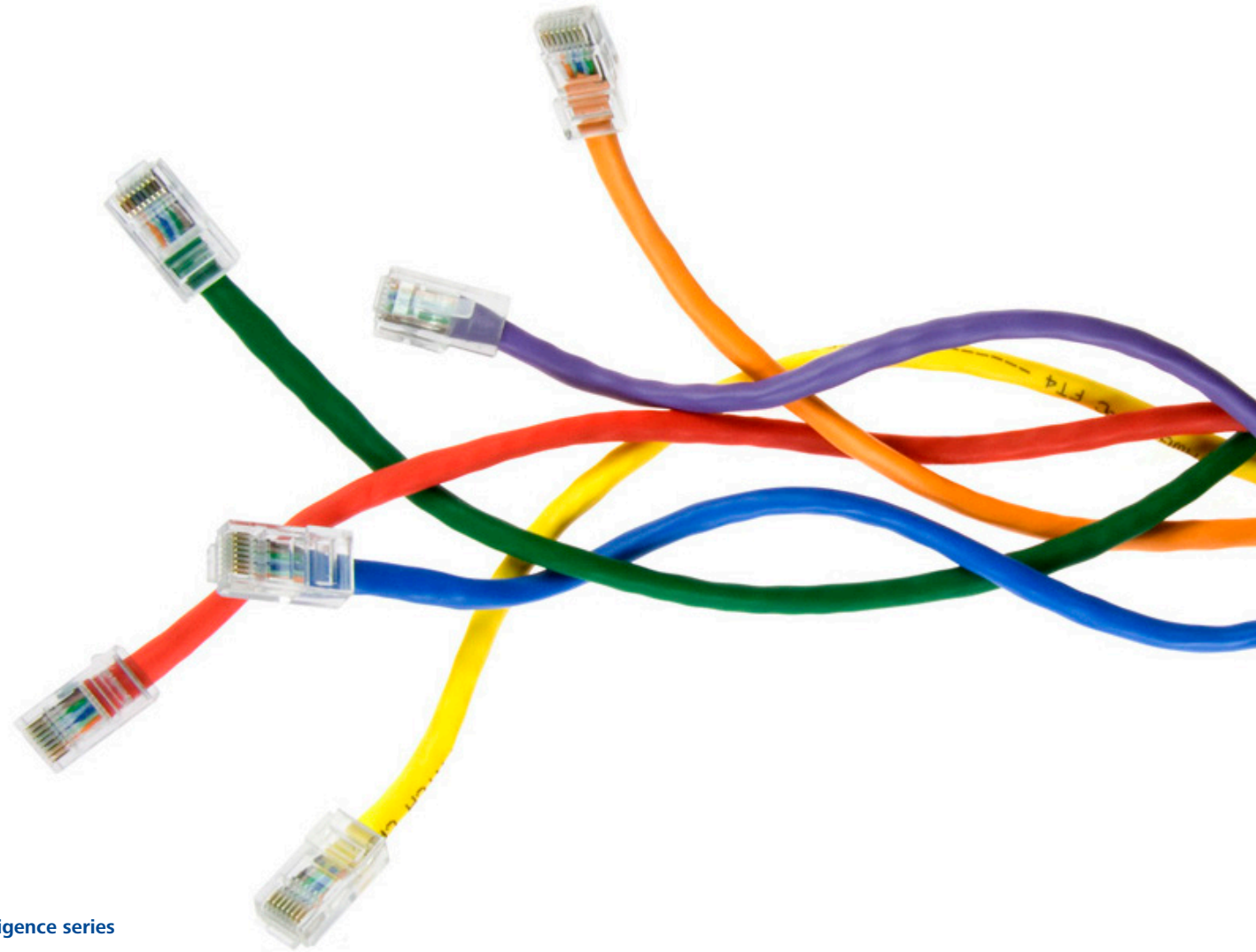
Deloitte.

Urgent convergence: Fostering Risk Intelligence in the Technology, Media & Telecommunications industries



Risk Intelligence series

Contents

Preface

This publication is part of Deloitte's series on Risk Intelligence — a risk management philosophy that focuses not solely on risk avoidance and mitigation, but also on risk-taking as a means to value creation. The concepts and viewpoints presented here build upon and complement other publications in the series that span roles, industries, and business issues. To access all the white papers in the Risk Intelligence series, visit: www.deloitte.com/risk.

Open communication is a key characteristic of the Risk Intelligent Enterprise™. We encourage you to share this white paper with your colleagues — executives, board members, and key managers at your company. The issues outlined herein will serve as useful points to consider and discuss in the continuing effort to increase your company's Risk Intelligence.

As used in this document, Deloitte means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

With convergence trends accelerating in the technology, media, and telecommunications (TMT) industries, what issue should be foremost in your — a TMT executive's — mind?

Perhaps not what you expect. Not mergers and acquisitions. Not product development. Not competition or outsourcing.

Rather, we believe you should pay close attention to … *physics.*

Yes, physics. In particular, we recommend a careful re-reading of Newton's Third Law, which states, "For every action, there is an equal and opposite reaction."

Within TMT, the action is convergence, which has industry boundaries vanishing and formerly distinct sectors coalescing. The opposite reaction, often unperceived, but lurking nonetheless, is intensifying risk. As TMT companies increasingly foray into new territory — untested markets, uncertain alliances, unfamiliar products — the risks facing them multiply exponentially.

Or, to put it in simpler terms: As sectors contract, risk expands. Action. Reaction.

TMT companies that fail to heed this fundamental lesson of physics may find another Newtonian principle comes into play — gravity — as they see their lofty aspirations for growth and profitability permanently grounded.

Enterprise risk mismanagement

Some TMT executives think, "Risk is not my problem." They consider risk management to be the domain of somebody else — perhaps internal audit or the chief risk officer or the chief compliance officer.

If that describes your mindset, here are a few questions for you: If integration with your recently acquired media company fails due to clashing corporate cultures, is it a problem for somebody else, or is it a problem for you? If your company is unable to accurately track revenue flow between your business partners, who's to blame? If your hot new electronics product can't be restocked quickly enough due to production problems with a key technology partner, who will ultimately be held responsible? When it's time to appear before the board of directors and explain such difficulties, who is going to take the heat?

If this is not convincing enough, other factors should put risk high on your list. For one, your world is getting more complex, with burgeoning globalization, expanding supply chains, increased outsourcing and offshoring, cross border M&A, and other factors all coming into play. For another, news outlets frequently report multi-million dollar judgments against companies that fail to identify risks pertaining to the unethical behavior of employees. Third, in many countries, regulators and financial exchanges (such as the SEC, PCAOB, and NYSE in the U.S.) all require or strongly encourage risk management activities; and institutional investors are increasingly demanding the same. At the same time, recent surveys show that CEOs rate risk management their number one concern. Another survey indicates that up to three-quarters of companies would scrap their entire risk management program and start over, if they could reasonably do so.[1] Meanwhile, boards and audit committees increasingly want assurance that their company's risks have been identified and are being managed.

How should you address these increasingly complex issues, intensifying regulatory pressures, and escalating stakeholder demands around risk management? We can summarize our response in two words: "Risk Intelligence."

The urge to converge

Several factors are driving the convergence of the TMT industry, most notably digitization, connectivity, and innovation.

Digitization: The move from analog to digital data is at the root of convergence, providing a uniform means of representing all types of information. In the pre-digital era, when words primarily lived on paper, images on canvas, music on vinyl, and even computer data on punch cards, no single device could accommodate it all. But convert all that information to digital form — ones and zeros — and suddenly a converged device that can handle it all isn't just

[1] Open Compliance and Ethics Group (OCEG), 2007 OCEG Governance Risk & Compliance Strategy Survey, Sept. 2007. www.oceg.org/view/GRCStrategyStudy

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.

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

Three levels of convergence

The Trillion Dollar Challenge: Principles for Profitable Companies (Deloitte Touche Tohmatsu, 2005), noted that TMT convergence is occurring at the following three levels:

1. Products and services represent the highest level of convergence, providing goods and services that meet real customer needs — above and beyond what is currently available. However, that result can only be achieved when supported by platform and organizational convergence at the other levels.
2. Platform convergence involves consolidation around a small number of standards — such as network protocols, data formats, and standard media types — allowing companies to focus their efforts, and creating critical mass in the marketplace. For example, adoption of the Internet Protocol (IP) as a universal standard for digital communication is fostering multiple convergent communication devices and applications.
3. Organizational convergence involves different companies' people and IT systems working together to deliver a convergent product or service. Since most convergence offerings extend beyond the capabilities of a single organization — no matter how large or diversified — convergence at the organization level is generally a prerequisite to delivering a convergent product or service.

The net effect of convergence is that TMT companies are becoming more and more intertwined in a tangle of content, technology development, and distribution partnerships. As these business models converge, TMT companies increasingly share responsibility for managing performance and risk.

a possibility, it's an inevitability. By distilling information into digital data, it can be viewed and manipulated using the same devices, technologies, processing techniques, networks, and media.

Connectivity: Wired and wireless networks are becoming faster and more pervasive: 60 percent of homes in developed countries are connected to the Internet; mobile voice and data networks now cover most major cities; and cellular mobile subscriptions now number two billion throughout the world.

This ubiquitous connectivity is fundamentally changing the nature of products and services. In the old days, once a product shipped from the factory, it was literally a finished product, with no way to increase its capabilities or value. Today, products are being designed with connectivity built in, allowing them to be remotely updated with new content, interactivity, and capabilities. (A prime example of this is the iPhone, for which Apple has promised periodic updates to enhance the phone's feature and functions.) Connectivity can compress the product lifecycle, enabling companies to deliver new features sooner, thus making the convergent offering more compelling.

Innovation: Technology continues its relentless advance. Observations such as Moore's Law, on the continual increase in computer processor speed, remain valid more than four decades since first postulated. Other key technology areas, including hard disk storage and solid-state memory, have also progressed steadily. Technology improvements make products faster, cheaper, smaller, and more energy efficient — allowing designers to pack more capability and features into a single device without making it unwieldy. Today's most powerful smart phones, for example, replace a whole roomful of separate devices and items — telephone, stereo, web browser, video player, calculator, photo album, appointment book, compass, alarm clock, and more — with a single product that fits comfortably in your pocket. Technology advances have helped drive the convergence trend, and will continue to do so, constantly redefining the limits of what is possible.

Promise and peril in TMT convergence

Chances are you don't need to be sold on the opportunities that arise from convergence. The trend is inexorable and the urge to converge nearly irresistible. Convergence at any level — platform, organization, product, or service — can create new market opportunities and new sources of revenue.

But let's be clearheaded. Every business initiative has its perils, and TMT convergence may have more than its fair share. Convergence can transform industries, inspire fundamentally new business models, restructure value chains, and shift the balance of power. All wonderful outcomes — if you're on the winning side.

To position yourself to take advantage of the opportunity convergence presents, you must be prepared to address the attendant risks. The chart on page 4 and the discussion that follows illustrate a few potential risks that TMT companies commonly encounter. This is not intended to be a comprehensive inventory of all conceivable risks (which, of course, would be impossible to produce). Rather, it is a representative sampling of possible risks that might arise.

Where's the risk?

What are the greatest threats facing your company? If you follow the money or monitor the media or track regulatory trends, you might assume that financial reporting risk is the greatest cause of executive insomnia. But recent poll data suggest such an assumption is incorrect.

According to a poll of more than 1,100 TMT executives taken during an August 2007 Dbriefs webcast,* risks to strategy and to operations/IT far surpassed financial reporting as the top concern. Approximately half of respondents cited one of these two risks; fewer than 10 percent named financial reporting.

* Dbriefs for Financial Executives, "Risk Intelligence in the Technology, Media, and Telecommunications Industries," August 22, 2007. Visit www.deloitte.com/us/dbriefs for more information.

A Hypothetical TMT company's top risks

Risk category	Specific risks
Strategy	• Complex business models • Merger integration • Intellectual property management • Partnerships/alliances
Operations	• Operating outside of core competencies • Business interruption • Risk of cascading failure
External factors	• Increased competition • Changes in customer demand and preferences • No control on consumer device • Emerging and rapidly maturing technologies • Blurring of competitive boundaries • Vulnerability of digital products and services
Legal	• Reputation • Anti-fraud/FCPA
Compliance	• Regulatory risk • Legislative wild card • Partnerships/joint venture investments
Finance	• Tax requirements • Revenue models
HR	• Retention of talent • Ethics/code of conduct • Succession planning • Complex management of • Distributed resources
IT	• Digital rights management • Infrastructure robustness • Security and privacy

Strategy

Complex business models. It's been decades since any company did it all — that is, conduct every facet of its business in house with its own personnel. But trends toward outsourcing, offshoring, partnering, and allying have accelerated in recent years. Take the typical personal computer as an example: one company builds the memory chips, another the hard drives, a third the network card. A Taiwanese manufacturer may produce the monitor, while a Mexican company creates the keyboard. Today, the value chain is more of a value web, with complex interrelationships among the parties creating a whole new set of risks.[2] Suffice to say, as your dependence on external organizations increases, their risks progressively become your risks.

Intellectual property management. TMT companies expend significant time and large sums on product research and development. This investment must be protected from patent infringement, theft, piracy, and other perils, often at great expense. Yet failure to protect can be even more costly, as the infringers erode market share and profitability.

Operations

Operating outside of core competencies. Just because you have built a profitable business in, say, manufacturing disk drives for computer companies, this doesn't mean you'll be successful in developing a line of MP3 players for consumers. Once you venture beyond your core competencies, a new world of potential hazards awaits.

[2] See "The Risk Intelligent Approach to Outsourcing and Offshoring" at www.deloitte.com/risk

External factors

Emerging and rapidly maturing technologies. Even if you do get your music player off the digital easel and onto the virtual shelves, are you ready to deal with the relentless pace of innovation and obsolescence in your new field? In some sectors, products are outdated before they even arrive in the marketplace.

Blurring of competitive boundaries. In the age of convergence, it becomes difficult to even identify the competition, never mind fend it off. For example, many cable TV companies have expanded beyond their "dumb pipe" origins to include TV program development, broadband Internet service, and telephone service in their menu of offerings. When yesterday's foe is tomorrow's partner, when companies routinely cast off one business model and quickly don another, competitive intelligence simultaneously becomes more arduous and more essential.

Vulnerability of digital products and services. The openness of the Internet, the interoperability of digital devices, and the ubiquity of digital data are simultaneously the strengths and the weaknesses of the digital age. The same systems that allow for unfettered delivery of enhanced products and services also provide a means for unscrupulous actors to engage in nefarious acts. This is not solely a security risk — it's an issue of digital asset management: how to protect intellectual property from being copied and transmitted around the globe and how to prevent unauthorized sale and use of that content.

Regulatory risk: A focus on privacy

One key risk area for companies in the TMT industry is managing the complex web of requirements regarding use of personally identifiable information. TMT firms must consider the risks and implications arising from their access to a variety of private data including customer billing and calling records, web searches and viewing habits, employee/HR records, and information shared with credit card companies and others. These issues are made even more complex due to the tangle of unique privacy laws that exist internationally and in the United States at both the federal and state level.

Compliance

Regulatory risk. As TMT companies merge and converge, unfamiliar regulatory requirements are often thrust upon the newly configured entities. Companies operating in multiple jurisdictions may face even more complex challenges. And organizations across most of the world need to pay constant attention to an evolving environment, as regulations are adopted, abandoned, and altered.

When your (Risk) eyes are bigger than your (Risk) stomach

Appetite and diet don't always harmoniously coexist. Sometimes hunger pangs go unsatisfied. Sometimes sated diners reach for dessert.

The same phenomenon can play out in the risk management realm. Companies can carefully define their risk appetite — how much risk they are willing to accept in pursuit of their strategic goals — yet still find themselves blindsided by a risk that they weren't even aware of. In other words, their risk appetite and their risk diet didn't match up.

And just like certain foods, if eaten in combination, can cause indigestion, different risks can combine or interact to create new and greater risks. For example, consider the hypothetical case of a financial services company that is managing its currency, interest rate, and cash flow risks. The company encounters a privacy risk — a stolen customer database — that it was unprepared to handle. Other risk issues rapidly come into play: reputational risk, litigation risk, and financial risk. Regulators get involved; ratings agencies get concerned; the cost of capital rises; investor confidence falls.

That's why it's so important to work methodically through the Risk Intelligence Framework. While perfection in risk management cannot ever be attained, the framework can improve the likelihood that risk events can be prevented or detected before they reach the crisis stage.

Human Resources

Ethics/code of conduct. Ethics, values, and the risk/reward relationship have become front-page news for TMT companies that "pushed the envelope" too far. (For reference, see recent news articles on stock option backdating and other offenses.) But even those that play fair are subject to the accelerating pace of change. Given the growing demand for and limited supply of talent, it is increasingly difficult to identify, attract, and retain staff with critical digital technology and content delivery experience.

Retention of talent. Many factors come into play in the talent "war," including the intense competition for workers in the U.S.; restrictions on accounting for stock options, which can hamper growth companies' recruiting efforts; and the "Google factor," which has Google recruiting a significant percentage of the top IT talent in Silicon Valley.

Complex management of distributed resources. The specialized knowledge required by TMT companies presents complex challenges and risks for getting the right people with the right knowledge and skills in the right place at the right time. In the face of the pressure to do this cost-effectively, many U.S.-based TMT companies have looked overseas, and in the process often unwittingly increased their "people" risks as they enter unfamiliar and less-certain labor markets. Another recent trend has been the increased use of contract labor and outsourcing — which shifts control of the talent pool but might not reduce the inherent talent risk. In fact, when these initiatives are poorly managed, the company exposes itself to yet more, not less, risk.

Information Technology

Security and privacy. Data breaches can carry significant reputational, legal, and financial consequences. Are you able to keep customer data secure? Do you have a means of identifying, sharing, protecting, monitoring, and tracking all forms of customer data usage?

The Risk Intelligence framework

The objective of the Risk Intelligence Framework is to ensure that the primary goal of an organization — the creation and preservation of value — is pursued in a risk-informed manner, and that risk is effectively managed in both a centralized and decentralized manner. The initial goal of applying the framework is to enable the company to identify its 10 or 20 most critical risks and respond appropriately. However, the same principles can be applied to all dimensions (and at all levels) of the organization — strategic, operational, financial, legal and regulatory compliance, HR, IT, and so on.

Embedded within each of the steps of the inner ring are considerations that are critical, yet not always widely observed. You may discover that you perform some of these steps well already, but it is the rare company, in our experience, that manages all the steps competently. Identifying which steps need further development will represent one of your first strides toward Risk Intelligence.

The Risk Intelligence framework

The Framework in action

To understand how the Risk Intelligence Framework wheel relates to the real world, we'll apply it to one of the TMT risk factors cited earlier: emerging and rapidly maturing technologies.

Innovation in TMT is relentless, providing both risks (e.g., being outflanked by the competition) and opportunities (e.g., attaining market domination with a creative new product). The pressure to innovate is inexorable, and no TMT company that hopes to thrive over the long haul can ignore it. Adopting the principles of Risk Intelligence can be a determining factor between success and failure.

1. ***Develop and deploy strategies:*** In this early planning stage, you first identify your company's strategic goals across a spectrum of business areas. Then, execution plans for attaining the goals are mapped out. For the purposes of our example, these goals will relate to rapidly evolving technologies. A consumer electronics company, for example, might set a goal of providing major upgrades of key products every 18 months; execution plans would be drawn up identifying the resources (financial, human, external, etc.) and steps necessary to accomplish this.
2. ***Identify risks:*** Next, you should systematically identify those risks that may thwart the attainment of your goals. This can be accomplished through various means, the most common of which is scenario planning. In this process, executives, risk managers, and other key personnel brainstorm around questions, such as: What risks could disrupt our plans? How vulnerable are we to these risks? In the case of emerging and maturing technologies, possible disruptions could include: (1) major technology breakthroughs by competitors; (2) insufficient resources devoted to research and development; and (3) rapid obsolescence of new products.
3. ***Assess and measure risks:*** In this phase, identified risks are assessed, measured, and prioritized. Take, for example, the three risks around evolving technologies cited above. Risk assessment activities may include intelligence gathering to determine the programs and progress of the competition; an appraisal of R&D to determine the adequacy of funding in relation to industry peers and market demands; and a market analysis to determine the need for shorter cycles between major product releases and upgrades

Note that these assessments may be conducted by different risk managers working in various business units. In such cases, it is critical that the bases for assessment are comparable. For example, we know of one TMT company that routinely conducted hundreds of risk assessments throughout its global operations. Aside from the information overload concerns, the assessments were performed using different methodologies and ranking criteria, making it impossible for management and the board to determine where risk management investments should be made. Such problems can be avoided by coordinating and consolidating the risk assessments.

Risk Intelligence ≠ ERM

Although a Risk Intelligent Enterprise addresses risks throughout the entire organization, that does not imply that Risk Intelligence is the same as ERM. Nor is Risk Intelligence "just another layer of risk management." Rather, Risk Intelligence represents a change in the way existing risk management functions work, collaborate, and think about risk. A Risk Intelligent approach never abandons existing capabilities and starts from scratch. Rather, it builds on the competencies and expertise that already exist within the organization. Risk Intelligence provides senior management and the board with better insight — better intelligence — on the company's exposure to risks and how they are being managed.

The rewards of Risk Intelligence include:

- Reduced burden on business operations
- Lower cost of risk management
- Improved ability to prevent, detect, correct, and escalate critical risk issues
- Means to improve strategic flexibility for both "upside" and "downside" risk scenarios
- Ability to provide a "comfort level" to the board and other stakeholders that the full range of risks is understood and managed.

4. ***Respond to risks:*** Various responses to identified risks are possible, depending on priorities, resources, risk appetite, and other factors. Options include seek, avoid, accept, transfer, and manage (see sidebar, "Risk Responses," on page 13).

   In our example, if the risk assessment determines that R&D is underfunded, the company may choose to increase the budget for in-house research; divert internal resources to R&D (with a neutral budget impact); partner with an outside firm to augment R&D; or invest in promising technologies being developed by other companies.

5. ***Design, implement, and test controls:*** Next, controls are put into place to allow you to prevent, detect, and respond to risk events. While in many cases, the most effective choice is prevention, an event may be beyond your control or ability to prevent. Then detection, response, and recovery come into play.

   Detection requires early warning systems to provide sufficient lead time for a response: the earlier the detection, the greater your ability to intervene successfully. Early detection also benefits risk taking for reward, as it gives companies the ability to recognize and take advantage of "upside" events. Many companies at this stage increase the role of technology by deploying automated controls, which offer the dual benefits of reducing long-term cost and improving effectiveness.

6. ***Monitor, assure, and escalate:*** Although many organizational hierarchies are possible, we recommend the following roles: Management ensures that risk controls are working as intended, and provides assurance to the board that risk is being managed within the defined risk appetite (see sidebar, "When Your [Risk] Eyes Are Bigger Than Your [Risk] Stomach," page 5). Meanwhile, internal audit provides reassurance to the board that management's assertions can be relied upon. "Ownership" of risk is maintained at the appropriate level, which may be within a business unit or geography; risk-related issues are escalated to management as warranted.

   In our example of the risks associated with emerging technologies, an outside law firm uncovers a competitor's patent application for a new technology that could render the company's product obsolete. The finding is escalated to management, which initiates a multifaceted response plan that includes finance (research possible acquisition of competitor); R&D (assess the viability of the new technology); and marketing (determine consumer appetite for this new product). These activities are presented to the board as necessary to let members know about the emergent risk and the actions taken.

7. ***Sustain and continuously improve:*** Once all the components of the Risk Intelligent Framework are in place, you should take steps to improve the efficiency and effectiveness of risk management. This involves a continuous process of harmonizing (ensuring that risk managers all speak the same language), synchronizing (coordinating across institutional boundaries), and rationalizing (eliminating duplication of effort).

   Applied to our example, the risks associated with rapidly evolving technologies would be regularly reviewed and updated by risk managers in various functions and business units. Their efforts would be coordinated throughout the organization, both to ensure that all contingencies are covered and that no unnecessary or unintended duplication of effort is taking place.

The outer ring: Governance, people, process, and technology

Governance, people, process, and technology form the foundations and infrastructure for attaining Risk Intelligence.

Governance — At the foundational base is a governance structure that recognizes the value of managing risks to create and preserve value. Defining and articulating the organization's tolerance for, and approach to, risk needs to be accomplished by the board, implemented throughout the various levels of management, and verified by internal audit. It is the foundation upon which all other infrastructure and processes are built and guides the board in conducting its required oversight of management.

People — Risk Intelligence is not about having a CRO or single centralized risk function, but rather is about changing the way the organization views and manages risk. Companies should provide role-based training that delivers risk management skills and awareness to the right people at the right time; as people move around an organization, it is imperative that they receive training related to the roles they are expected to perform in a timely manner. Generally, this is an ongoing process, not a "once and done" event. The corporate philosophy around risk-taking needs to be articulated and embedded into how people do their jobs, and this requires training and monitoring of results.

Processes — A Risk Intelligent approach establishes commonality and linkages between risk management processes — establishing risk appetite at the corporate level, translating and cascading thresholds throughout the organization, and ensuring a consistent approach to managing and reporting. The Risk Intelligence Framework is also about integrating Risk Intelligence and consistent risk management activities into mainstream planning, management, and operational decision-making processes at all levels. Recognize that the steps in the inner ring apply not only to the corporate risk management process, but also need to be embedded into mainstream processes to ensure that Risk Intelligent planning and management do in fact become part of everyone's job. The corporate risk management process is critical to understanding risk interdependencies and to managing risk more holistically.

Technology — In the most savvy companies, technology plays a key role in risk management. Software tools that provide controls monitoring and "dashboard" views are dynamic and evolving rapidly, with new and enhanced capabilities being continually developed. Technology can be leveraged to provide common platforms for identifying, measuring, reporting, and monitoring risks; there are presently a number of current and emerging solutions, including "GRC" suites from leading ERP providers. These provide an opportunity to rationalize and automate controls across silos and risk management domains, thereby increasing both the effectiveness and efficiency of controls.

GRC defined

Much confusion exists in the marketplace about the term "GRC" — governance, risk, and compliance. Some equate it with computer software applications; others consider it synonymous with corporate governance practices. We believe it is all of these things — and more.

Rather than considering the components of GRC in isolation, we recommend a broader, more encompassing, *Risk Intelligent* view that acknowledges and understands the interdependencies of the three areas. The fact is, you can't attain good governance without paying attention to regulatory compliance; nor can you achieve compliance without addressing the attendant risks. Since the three areas don't exist independently, we believe it makes eminent sense to take an integrated, Risk Intelligent approach to addressing them.

A Risk Intelligent approach to GRC can provide an integrated, enterprise view of the many governance, risk management, and regulatory compliance challenges facing your organization.

This approach can improve your company's ability to anticipate and proactively respond to emerging risks; and can help reduce silo-based activity, redundancies, excessive costs, and ineffectiveness.

Risk responses

Once risks are identified and assessed, you must decide how to handle them. Here are some options:

Seek — Intelligent risk taking is fundamental to business success. Yet risk aversion persists. For example, some large media companies are so concerned over digital rights management that they have not made their content available online. This stance has had the ironic effect of providing incentive to consumers who want their content electronically to resort to illegal methods, thereby costing the company revenue. Conversely, those companies that have sought out the opportunities and addressed the risks in digital delivery have developed viable business models and substantial customer bases.

Avoid — Risk avoidance is a common response. For instance, some telecoms are choosing not to enter certain markets because of perceived geo-political risk concerns. Factors such as social unrest, political instability, unfriendly regimes, war, insurgency, and terrorism can all come into play. In addition, poorly developed or maintained infrastructure, inadequate education, corruption, immature markets, and other concerns might dissuade companies from expanding into particular markets despite tremendous upside potential.

Accept — Of course, there are always exogenous risk factors that one just has to accept. For example, after spending billions laying fiber optic lines, telecom companies may face the risk that consumers choose not to purchase advanced features and applications from the telecom company and only purchase broadband service from the pipe. Significant value resides in the applications, and other firms can sell the applications without investing in the infrastructure.

Transfer — When risk exposure falls outside a company's risk appetite, or when an organization desires to eliminate surprises or smooth out costs, risk transfer activities come into play. Insurance and futures contracts are two of the most common approaches to risk transfer. Companies should make certain that the transfer of risk matches their expectations. For example, computer consultants and software developers who take out errors and omissions insurance should carefully scrutinize any coverage exceptions.

Manage — Intelligently managing risk is, of course, the most important strategy of all. For example, telecom companies have been facing a spate of class action lawsuits on a wide variety of consumer protection issues, ranging from allegations that they have overcharged customers fees and taxes to lawsuits about failure to disclose wireless coverage limitations. A Risk Intelligent approach might recognize the vulnerability of companies to increased scrutiny from regulators in the wake of such highly publicized lawsuits and take action to meet such threats. For instance, legislators and regulators have been concerned about early termination fees imposed by wireless carriers. A number of wireless carriers chose to manage that risk by recently announcing they would prorate such fees when customers transfer to another carrier.

Evolving into a Risk Intelligent TMT company

Establish an enabling environment	• Identify champions throughout the enterprise. • Communicate and enforce authority and accountability for risk decision making. • Reinforce "tone at the top" through good governance, codes of conduct, andstatements of shared value.
Achieve enterprise-wide coverage	• Employ risk management activities that encompass all material risk types and business units. • Implement hybrid approach employing the best of probability and vulnerability based techniques.
Take advantage of portfolio effects	• Adopt a portfolio view of risks that naturally offsets risk exposures. • Measure risk exposures from both the top down and bottom up to become fully Risk Intelligent.
Incorporate risk into strategy	• Evaluate risks at various levels, from the overall enterprise level through to the business unit,project, product, or even the transaction levels. • Use new metrics to integrate risk with performance management.

Risk Intelligent Enterprises that are most effective and efficient in managing risks to both existing assets and to future growth will, in the long run, outperform those that are less so.

Making the Risk Intelligent choice

To excel in converging markets, your TMT company must consider risk in new ways and must address risk aggressively. As you expand beyond your traditional domains and move out of your comfort zones, you can enhance your prospects by adopting the principles of Risk Intelligence. This will enable you to move beyond assessing and reacting to anticipating and proactively responding to risks. Risk Intelligent companies manage risk-taking for reward as aggressively as they manage risks to existing assets.

The process may seem daunting and, indeed, attaining Risk Intelligence is a major undertaking. However, just as with any major initiative, small steps can yield big results. Don't bite off too much at one time; rather, start with the areas of greatest vulnerability (those that will impact your share price if risk becomes reality) and work your way down the list. Handled in this manner, your journey toward Risk Intelligence becomes more manageable and navigable.

Make no mistake — the landscape is shifting in the TMT space. Those companies that can capitalize on key trends and opportunities, while recognizing, taking, and managing risk, will more effectively position themselves for long-term success.

For more information

Where do you go from here? Most organizations will benefit from our complete Risk Intelligence whitepaper series that provides benchmarks and a roadmap for addressing the governance, people, process, and technology how-to's of effective risk management. The series, now supported by the new Risk Intelligence Map, provides perspectives on Risk Intelligence from industry and functional viewpoints. Visit www.deloitte.com/risk to access the full series of papers.

Risk Intelligent questions to consider

- How much could we lose if we don't manage this risk intelligently?
- What is the likelihood of the risk occurring?
- What is our vulnerability to this risk?
- Is the risk correlated with other risk exposures?
- Does this risk represent a concentration of risk that may cause problems in risk management or mitigation?
- If I hedge or mitigate this risk, how does this change the likelihood and impact?
- Does our risk management or mitigation strategy introduce any additional risks?
- How much can we gain if we take this risk — provided we manage it properly?
- How can we get assurance that our confidence is justified?
- How much is it costing us (or will it cost us) to manage this risk?
- Is there a potential reputational risk impact from this risk?
- What individual or team is responsible for managing this risk end-to-end?

Contact us

To learn more about Deloitte's governance and risk services or to contact one of our global leaders, please visit: www.deloitte.com/risk.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, 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 shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2013 Deloitte Development LLC, All rights reserved
Member of Deloitte Touche Tohmatsu Limited