Smart moves
Manage risk effectively in four critical areas

Deloitte.
## Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Of risk and reward</td>
<td>1</td>
</tr>
<tr>
<td>Deloitte Risk series</td>
<td>2</td>
</tr>
<tr>
<td>IT risk: get with it or go home</td>
<td>3</td>
</tr>
<tr>
<td>Cybersecurity remains a growing problem</td>
<td>8-9</td>
</tr>
<tr>
<td>Contract risk and compliance</td>
<td>16</td>
</tr>
<tr>
<td>Internal Audit</td>
<td>21</td>
</tr>
<tr>
<td>One step at a time</td>
<td>25</td>
</tr>
</tbody>
</table>
The constantly accelerating pace of change requires organizations to keep moving forward – no matter what. After all, few leaders will say the secret to sustained business success is about resting on your laurels. The rewards of constant organizational evolution are clear, and sometimes the risks are great. But the risks of standing still? Those are even greater.

If you’re to move forward safely and securely, then, intelligent risk management is paramount – whether that means finding new ways to boost value or recover costs, implementing better approaches to cybersecurity, or adopting the newest technological innovations to improve client satisfaction.

The role of risk professionals, executives and all those responsible for protecting their organization is therefore only going to expand as innovation continues to disrupt the way business has long been conducted. And as Deloitte’s 2015 report on Canada’s productivity, The age of disruption, revealed all too clearly, most of our companies aren’t ready to handle it.

But organizations can prepare for disruption. They can begin by ensuring risk is managed as effectively as possible, creating new value in the process.

This paper explores the emerging trends, challenges and best practices in four key areas: information technology, third-party risk and compliance, cybersecurity and internal audit. These areas were the focus of Deloitte’s most recent Risk Series (2014-15), in which we held seminars across Canada to share the perspectives of Deloitte experts and spark conversations with business leaders about key matters facing businesses. (We also polled participants about their organization’s approach to risk management; look for some of the results throughout.)

Most importantly, this paper offers direction on what you can do to help protect and enhance the growth of your organization as it moves toward the future. We hope you find it useful.
Assessing risk is an ingrained human trait. Millennia of evolution trained us to evaluate the prevalence, immediacy and severity of threats. We then respond in an appropriate manner, expending the optimal amount of energy for a given situation. It’s a system that works.

Over time, threat evaluation evolved to include social structures and alliances to help groups stay safe in environments that include ambiguous and novel threats. Deloitte’s Risk Series applies those principles to modern business. Because today, disruption and threats come from all angles, with entirely new guises and requiring very different responses. Every business can use help to scan its environment, identify potential danger and prepare a plan of action to protect itself and spur future growth.

**Deloitte’s 2014-15 Risk Series offered solutions in four critical areas**

**Information Technology: Time to brace for emerging disruptive technologies**
From analytics to artificial intelligence, both current and emerging technologies present incredible opportunities that can help organizations grow in leaps and bounds. But those who embrace them must also be careful about opening the door to risk as well as to benefit. Traditional protective measures are still fundamental to managing technology risk but they need to be supplemented by broader measures that can adapt to the accelerated pace of innovation. A company’s finances, reputation, data and regulatory compliance depend on it. General computing controls are important, but the real challenge is shifting IT risk management and audit focus towards high value areas that are also high risk.

**Cybersecurity: Learn the lessons or pay the price**
By now, everyone recognizes cyberattacks threaten any organization. So for all intents and purposes, the concern is universal. In Canada, 36% of Canadian companies reported being attacked and cyber crime cost Canadian businesses more than $3.2 billion in 2013. Cyberattacks carry price tags that can run into the hundreds of millions of dollars for individual organizations, and potentially incalculable reputational harm. The question to ask is: how can you protect your workplace, customers and networks?

**Contract Risk and Compliance: Greater transparency delivers greater value**
Wouldn’t it be excellent if there were a way to simultaneously improve your organization and its relationships with third parties? That is what Contract Risk and Compliance (CRC) is all about. In a business world increasingly marked by multiple outsourced vendors, suppliers and partners, CRC helps ensure all parties fulfil agreements to maximize value for everyone. A formalized process to verify adherence to contract terms and compliance with regulatory requirements among all parties minimizes risk exposure. It also increases trust and cooperation by clearly stating expectations of all sides.

**Internal Audit: Adding value in a changing landscape**
An accelerating rate of change is an accepted fact of life in the modern business world. Our connected global economy requires flexibility on all fronts, particularly when it comes to managing risk. For most companies, Internal Audit (IA) is a critical bulwark against internal and external threats. But the rapidly shifting business landscape is heightening expectations of IA. This is especially true when it comes to adding value by delivering such items as flexible audit planning, scrutinizing emerging risk and employing data analytics to improve business outcomes. Of course, all of this must be accomplished while striking the right balance between the traditional assurance role and an advisory focus. Is your IA department ready to take on this tall order? If it is, is your organization ready to let it tackle this vitally important job?
Staying current is a rule of staying relevant. When a new best practice makes its appearance, organizations either jump on board or watch business go elsewhere. Every advance from the industrial revolution through the assembly line to the rise of digital has spread quickly, thanks in large part to the willingness for early adoption. But when it comes to Information Technology (IT) risk management, the currency imperative somehow seems to lag for too many organizations.

That, unfortunately, is as true in Canada as elsewhere in the world. In general, our companies aren’t ready to handle the technology tsunami that’s coming. The early markers show it will usher in new era of business disruption and, in the process, open a Pandora’s box of risk.

Traditional concerns over passwords and other protective measures are still fundamental to managing technology risk but they need to be supplemented by a much broader view of risks and protective measures. The finances, reputations, data and regulatory compliance of organizations depend on it. General computing controls and regulatory requirements are important, but the real job is helping organizations manage risk by shifting IT risk management and audit focus towards high value areas that are also high risk.

These “high value, high risk” areas of IT risk can be divided into two categories: those that exist today and those that are emerging.
From protecting against increasingly insidious cyberattacks to keeping a close watch on the data used in analytics, managing the technology risks in play today is complex and constant, requiring ongoing vigilance to keep pace with developments. Organizations can further mitigate risk by implementing a strategic, comprehensive framework to ensure a “big-picture” view of their IT risk management. They should also strive to keep control of the message when – not if – they have a damaging breach by having a robust crisis management and communications plan ready to roll out immediately.

The main IT issues challenging risk professionals today include

Cybersecurity: Pass the test
In too many cases, attack and penetration tests represent a complete cybersecurity posture assessment. As long as the firewall is set up to keep out bad guys, they feel confident in their defenses. Attack and penetration tests are, in our view, extremely valuable but they’re just one piece of a framework that can help make organizations secure, vigilant and resilient. Proactively identifying and monitoring for potential actors, motives and attack vectors and how it may impact your business helps address the ever changing threat landscape. Establishing such a framework should begin with a multi-year risk management and audit plan that covers all cyber domains. The plan should include an execution schedule that considers all relevant checks and balances.

Third parties: The extended enterprise
Increasingly, organizations are using third parties to deliver services. Our interconnected world requires them to know which security measures their outside service providers (OSPs) employ. Organizations first need to know all the OSPs they use, which involves not only taking an inventory but also identifying to which cloud-based service providers information packets leaving the organization’s network’s are headed and are being reviewed in the accounts payable system to find which OSPs are being paid. With a complete picture of all the third parties it’s involved with, an organization can then perform a risk assessment in order to manage their OSPs in a more risk-intelligent fashion. Too often the view is that the responsibility for an outsourced service belongs to the OSP, but the reality is that the organization holds the ultimate accountability for risk and control.

Data: To store and protect
Whether it’s OSPs or internal business units, data is a high priority for most organizations. Data whips around via increasingly interconnected networks, email, mobile devices and social media. It’s the lifeblood of business and it must be protected. We believe securing data must go beyond mere storage. It requires active management through the four key stages of the data life cycle: acquisition, sharing, use and destruction.

Management is no easy task: data and privacy regulations differ across jurisdictions and cover everything from who can see data and how it can be used to how long it may be kept and when and how it must be destroyed. Data security involves knowing not just what’s getting inside your firewall and how it’s protected, but also knowing what data is leaving your domain and ensuring that it is authorized and protected. Outbound monitoring is critical.

Managing risk starts with defining organizational policies, understanding relevant regulations and evaluating how your controls measure up in areas such as data ownership, protection, record-keeping, personal device use and data destruction.
Social media: Post haste
Every moment, organizations purposefully share data through social media. This entails risk. Younger professionals have grown up with a comfort in having information on social media that is sometimes at odds with organizations’ desire to share information on a need-to-know basis. Therefore, we advise moving to a program-level view of the risk presented by social media. With the blurring of lines between work life and personal life, this view must extend to personal activity as well.

The program should encompass the integration points of various social media, crisis management plans and compliance issues, as well as social media policy development in areas such as legal and human resources. Staff must be provided clear guidance on what is acceptable use of social media and what restrictions there are in regards to the organization’s information.

Analytics: Big data on demand
Organizations are increasingly leveraging the growing base of data available to them and using analytics to make better business decisions. Understanding these decisions is a good place to begin understanding the potential risks. For example, algorithms that place banner ads are unlikely to imperil a company’s existence, while those that place billion-dollar trade orders just might.

Organizations must know what data is being used and what it’s being used for, particularly if this usage might have a material impact on a business. Data quality matters, too: quality control of the information being fed into data analytics must be examined to ensure that decisions are based on complete and accurate information. A failure to do so needlessly increases risk.

Managing the risks of existing technologies is enough to keep those responsible busy more than full-time. But they must make time to look ahead because technological advances are raising the risk stakes at the same time as heralding unprecedented new opportunities for growth. The vast majority of organizations are not spending enough time considering the far-reaching ramifications of disruptive technologies.
How disruptive technologies are changing the game in risk

Science fiction is becoming science fact. There is a wave of so-called disruptive technologies on the near horizon that promise to have a great impact on our personal lives and our business practices. Very recently we have seen the advent of driverless vehicles, wearable devices with the capacity we previously enjoyed in large computers, as well as computers that are increasingly able to make decisions based on “learning” from past decisions and experience. Estimates suggest that by 2017, the world will be adding a trillion sensors per year, ushering into existence a fully functioning Internet of Things.

This wave of change will bring new challenges for risk professionals as the risk universe expands and the speed of exploitation becomes ever faster.

This article will focus on five areas of technology where great leaps forward are not only theoretically possible but are, in fact, already happening. They are:

- Wearables
- Drones (self-piloted/remotely piloted devices)
- Open-source technology
- Artificial intelligence/cognitive computing
- Sensor proliferation

These technologies will have a fundamental impact on how we do business and have potential to be disruptive in the marketplace. A recent Deloitte Consulting study, The age of disruption, identified that the majority of Canadian business organizations are not well prepared to profit from or cope with this coming wave of new technologies. As those responsible, directly or indirectly, for managing risk in our respective organizations, we need to go beyond knowing which technologies are coming next. We need to understand the impact these technologies will have and address the readiness of management to manage these opportunities and the attendant risk. A good starting point is looking at the various types of risk these technologies can create.

Security risks
As soon as data is digital, it’s vulnerable. We are already in an environment where our data and systems are vulnerable to cyber threats. As sensors proliferate, as increasing reliance is placed on decisions based on advanced cognitive computing and as our systems and data are resident in sensors, wearable devices and drones that will reside outside the traditional bricks and mortar of our organizations the threat of cyber-attacks and exploits will also proliferate. Increasingly intellectual property and personal identifiable information will be transmitting through cyberspace, along with financial data and other information that will be attractive to cyber criminals.

Protecting this information is clearly a paramount concern and the scope and strength of cyber defences will need to advance apace with the new technological advances.

Physical risks
Any technology that moves things creates some degree of risk. All five of the above-listed technologies potentially impact the way items move. Robot lawnmowers, automated warehouses and self-driving big rigs could all be in our collective future. Of course, there’s a big difference in the risk potential between a driverless forklift that suddenly shuts down and an out-of-control 18-wheeler careening across a highway.

Decision risk
As management functions are farmed out to computers and automated processes, the question becomes what happens when mistakes are made? Artificial intelligence that improperly stocks a refrigerator is a very different risk than a robot doctor that “reads” body scans and makes a diagnosis. If a computer is guiding decisions, what controls are in place to make sure those decisions are ultimately correct and ethical?

Support risk
As is always the case with new technologies, some endure, others fall away. Those responsible for managing risk have to examine their organization’s reliance on these emerging technologies and how prepared they are to either support their development or, if necessary, find alternatives. This is particularly true when it comes to open-source technology that depends on participants to develop it leading to concerns about change management and indeed ownership of the software asset.
Regardless of the technology or the risk it creates, our most critical job is ensuring we ask the right questions of the right people involved. The first step is to understand usage and anticipated adoption in your particular field. Obviously each sector will incorporate different aspects of technologies in different ways. Getting a handle on how technological advances are going to be used in your space is an essential first step.

Once you know how the various technologies are most likely to be applied in your field, determine the events they will impact. Will cognitive computing replace human decisions in some area? Will connected sensors tell machines when to stop and when to go? Is your computing architecture going to be based on source code developed by an army of open source participants? The answers to these questions will guide the areas of risk you must assess.

Senior executives will have their own questions. How will these disruptive technologies impact the business marketplace and will new competitors emerge? What are the specific legal risks of the applications of new technology in our business and sector? Does it create conflict with other stakeholders? Identifying these questions is essential to getting answers.

Clearly, emerging technologies present incredible opportunities that we can use to our great advantage. We must be vigilant about opening the door to risk as well as benefit, and create a solid plan to protect our day-to-day business operations.

A final pair of thoughts for all of us to consider: Firstly, these new technologies are not arriving one at a time. While their application will differ across sectors and vary greatly depending on organizational maturity, we will be dealing with multiple technology advances concurrently. The interconnectedness of so many digital data points makes data analytics ever more important as a tool to manage this proliferation.

Secondly, we must consider the cascade effect these developments create. There will be increasing interdependencies between technology advances and one unchecked risk could lead very quickly to other unanticipated consequences.

These will be exciting times and the need for proactive and intelligent risk management will be greater than ever. Enjoy the ride!
Every week seems to bring news of another organization experiencing a cybersecurity breach. Within the last two years, some of the biggest names in retail, manufacturing, consumer business and telecommunications have made the wrong kind of cybersecurity headlines. The cost of these incidents routinely runs into the hundreds of millions of dollars. That is on top of sometimes incalculable reputational harm.

In 2013, cyber-crime cost Canadian businesses $3.2 billion¹ and 36% of Canadian companies reported being victims of a cyberattack². It’s not just businesses that are at risk. As the theft of employee personal information from a federal U.S. bureau in spring 2015 proved, personal data can also be attractive. So can information about critical resources such as water. With its abundance of natural resources, Canada could move into multiple target scopes when global supplies start running low. And Canada’s position as a next-door neighbour enjoying a good relationship and some common infrastructure with the U.S. may make it an attractive entry point to infiltrate the superpower.

One of the biggest cybersecurity challenges for many Canadian business leaders is determining how, on a functional level, to bridge the gap between the technical side of the equation and the business side. Those making the technical decisions may not fully understand what goal the business stakeholders want those technologies to achieve, while the stakeholders may not realize what the technological tools really do. Determining exactly how to align the tools and the business strategy to protect the organization is key.

It’s not just businesses that are at risk
Identifying your organization’s potential attackers, their targets and techniques are vital first steps. Behavioural analysis aimed at understanding the motivations behind specific potential threats to your organization can help you focus on your areas of greatest concern.

In public sector areas such as healthcare and education, client confidentiality is a top priority. The retail and financial sectors must zealously guard payment data and account information, and most industries have trade secrets or proprietary knowledge to protect. Knowing what cyber criminals are likely looking for—or motives why they may want to disrupt your business can assist you in deciding how to allocate precious resources.

A good starting point for any organization are Deloitte’s five steps to improve cybersecurity. They are

- **Focus on what matters:**
  - your crown jewels and relationships
  - Understand critical assets and interactions.

- **Proactively assess your cyber risk**
  - Know what to look for and how to detect threats – whether conventional or emerging.

- **Focus on awareness to build a multilayered defense**
  - Develop a cyber program that addresses a combination of defenses for your organization, employees, customer and partners.

- **Fortify your organization**
  - Have a plan to patch holes, manage patches, develop software securely and address physical security.

- **Prepare for the inevitable**
  - Focus on incident management and simulation to “test your gates” and your response.
It’s about time

Preparation is especially important given the speed and sophistication of today’s cyberattacks. At present, many breaches go undetected for extended periods of time. The focus should be targeted on proactive detection. In the past, detection programs could root out signature-based malware. Modern asymmetrical attacks are harder to identify. Social attacks and credential theft are on the rise, and destructive code can idly sit inside networks for days, weeks, months or years until it starts wreaking havoc. In today’s online world, 100% security is impossible, but detecting malicious patterns and suspicious behaviour is a critical starting point for everyone.

More troubling is what happens once an attack is underway. A 2014 Verizon study, analyzing 63,000 security incidents in 50 global organizations, revealed some startling facts, including:

- 72% of initial compromises occur within minutes
- 46% of data leaks occur within minutes
- 72% of attacks take weeks or longer to discover
- 59% of attacks take weeks or longer to contain

In very simple terms, systems are frequently compromised within minutes. Sometimes it takes just seconds. Meanwhile, detection and mitigation usually take weeks, months or more. That kind of math does not inspire confidence.
People problems

Organizational boundaries are blurred by “bring-your-own-device” policies and partnerships

Nine basic patterns account for 92% of all incidents. Web application attacks, cyber espionage and point-of-sale intrusions are the three variations which, on average, account for 72% of all hacks. But people remain the weakest link in the security chain. As such, they are increasingly the targets to begin attacks.

Nefarious intent from insiders is not required to put networks at risk. Errors and omissions such as failing to update a security patch can cause massive harm. Deloitte’s own readiness testing of clients illustrates the problem. Our teams sent client employees “spear phishing” emails designed to resemble common cyberattacks. About 65% of users opened these messages and roughly a third actually provided credentials in a response. Clearly, awareness remains a work in progress. Organizational boundaries are blurred by “bring-your-own-device” policies and partnerships.

Most alarming are all-too-frequent examples of people gradually coming to accept cybersecurity red flags as normal. In two of the most high-profile attacks in recent years, people identified – and then ignored – obvious warning signs. Adequate responses could have eliminated or contained the damage in each case. But instead of building intelligence from these indicators, they were treated as minor blips. The organizations continued metaphorically inching towards a cliff. Eventually, each one suffered a hard fall. Businesses must prioritize responding to and learning from these warnings to prevent groupthink from having catastrophic consequences.
Another crucial measure is involving entire organizations in cybersecurity planning. Going beyond Risk and Internal Audit to include departments such as Legal is essential. Often when cyberattacks involve third-party data, first responders must wait to get a legal opinion before they can begin to act. The result is like having firefighters arrive at a burning building, only to turn off their hoses while waiting for lawyers to chime in. Establishing legal frameworks before an incident occurs can help ensure more effective containment in a crisis.

Simply keeping up with evolving regulations is a full-time job, one that diverts scarce resources away from cyber threat management. Keeping pace with the increasingly sophisticated technologies and methods of cyber attackers is another time-consuming but necessary task. This can be achieved through building strategic relationships with specialized companies, collaborating with peers in the cybersecurity community and “thinking like a burglar” to analyze your organization’s assets and weak links more objectively.

What’s critical in the fight against cyber threats is an organization’s ability to find the right operating model to be more secure, vigilant and resilient. Cost and business imperatives will drive the right operating model whether you insource, outsource or co-source your cyber defenses.

**But all prevention models must deliver on three key metrics**

- **Security** - fundamental, effective information controls.
- **Vigilance** - proactive threat monitoring that looks for patterns and behaviours; intelligence gathering including cyber chatter and updating threat scenarios and technology.
- **Resilience** - preparing to contain any type of breach and continually updating response policies, testing with simulations and developing dynamic recovery plans.

Despite the very apparent risks, attitudes towards cybersecurity often remain “It doesn’t happen here. It doesn’t happen to us. It doesn’t happen to me.” Too many companies, including more than a third of Canadian ones, already know better. The reality of cyberattacks is a matter of when, not if. So what organizations really must ask is if they prefer preparing before an attack happens or paying dearly to clean up after one occurs?

A third option – eschewing cyber altogether to eliminate all associated risk – is not viable, nor even desirable for the majority of organizations that already depend on the business advantages technology offers, from the smallest of daily operations to opportunities to provide advanced products and services that were unimaginable even a few years ago. Cyber is an enabler for growth: make it part of your business DNA. Just make sure it includes a robust defence system.

---


3 Verizon 2014 Data Breach Investigations Report

Do our board and C-suite demonstrate due diligence, ownership and effective management of cyber risk?*

A 31% Board and C-suite hold a C-level executive accountable for cyber threat risk management and are responsible for overseeing the development and confirming the implementation of a cybersecurity program

B 37% Leadership and board oversight are concerned with cybersecurity issues, but stakeholder communications and oversight of specific structures remain largely high level

C 12% Tone at the top lacks cybersecurity focus and understanding of strategic issues

D 14% Little engagement by leadership in specific IT security issues

E 6% Don’t know

Can our organization rapidly contain damages and mobilize diverse response resources should a cyber-incident occur?*

A 8% Clear reporting and decision paths exist for action and communication in response to a security failure or accident

B 10% Crisis management and cyber security incident response plans and procedures are documented and rehearsed through war gaming, simulations and team interaction

C 48% Basic cyber incident response policies and procedures are in place but not effectively integrated with existing business continuity management and disaster recovery plans

D 23% Cyber incident policies, response plans and communications are minimal or non-existent

E 11% Don’t know
How do we evaluate the effectiveness of our organization’s cyber security program?*

A 17% The board, or a committee of the board, is engaged on a regular basis to review and discuss the implementation of the organization’s cyber security framework and implementation plan, including the adequacy of existing mitigating controls.

B 28% Basic cyber security assessments take place on a fixed, unvarying schedule and are not industry specific.

C 19% Internal audit evaluates cyber risk management effectiveness no more than once a year.

D 24% Cyber security assessments and internal audit evaluations are sporadic or non-existent.

E 12% Don’t know.

* Polls taken by participants at a 2015 Deloitte Risk Series seminar. Percentages rounded.
Imagine driving a car onto a highway, choosing a lane and then setting the cruise control with no plans to monitor the road until you reach your destination. It sounds more than a little reckless. But too often, that’s the approach businesses take to Contract Risk and Compliance (CRC). It’s especially dangerous given how common it is today for companies to rely on extended business models defined by multiple, outsourced, third-party relationships.

These relationships, even in organizations with a strong risk focus, frequently reside at the edge of – or outside – the risk umbrella. An “out-of-sight, out-of-mind” attitude is often adopted once a company delegates a service to a vendor. After signing a contract, many executives assume all parties will perform as expected, or that relationship management and risk monitoring mechanisms are in place and functioning properly. Canadian organizations in particular might be a little more trusting of their external service providers and perhaps less challenging when something not quite right happens; we do have that reputation for being “nice”. But just like drivers who continually scan the road so they can appropriately react to changing conditions, businesses – Canadian ones, too – must constantly monitor and re-evaluate the environment in which they operate.

This is particularly true when it comes to CRC, where every party to a contract is akin to another driver of whom you should be aware. Greater transparency in CRC within your extended business model means enhancing an organization’s ability to see into itself. It means fully understanding your contract portfolio and third-party relationships across the enterprise to actively manage contracts, assess their value, ensure compliance and minimize risk. Active management and monitoring of third parties can also prevent money from falling through the cracks. We typically find 3% to 5% in recovery opportunities and process cost savings on major capital spend projects. That’s $3m to $5m on a $100m contract, no small change to reclaim from the table – if you know it’s there.

Vendor governance is frequently spread across various internal stakeholders and departments, preventing a complete overview of the corporate contract structure, discouraging holistic management and leading to a compliance approach that is reactive and reparative rather than proactive and preventive. It is rare to see an organization appoint one person to be accountable for the holistic view of third party vendors, but the benefits of doing so may be worth considering: to effectively manage risk, you need a full picture of your extended organization. That means analyzing Key Performance Indicators (KPIs) of critical vendors and regularly reviewing contracts to extract maximum value from third-party relationships, which may include manufacturers, suppliers, service providers, joint ventures, distributors, licensees, agents, franchisees and affiliates.
Maximizing contract value while minimizing risk requires that contracts be effectively managed across three critical phases

Initiation
- Determine the contract type (revenue share, license fees, intellectual property, etc.) and commercial structure (fixed price/lump sum, cost reimbursable or unit price).
- Create and maintain the contract by capturing key requirements, developing the contract, achieving sign-off and execution, and retaining the contract appropriately.
- Incorporate KPIs and Key Compliance Indicators (KCIs) into the contract to improve visibility, agility, consistency and performance.
- Include a robust “right to audit and inspect” clause.

Administration
- Understand the range of existing contract (document) management competencies and work to improve them in your organization.
- Make effective use of contract management tools.
- Carefully consider whether your contract’s KPIs and KCIs support strategic objectives, and recalibrate/renegotiate as appropriate.

Compliance
- Enhance contract clarity and transparency through regular communications and check-ins with your vendors.
- Maximize cost recoveries and future cost savings by analyzing data from end to end in the procure-to-pay life cycle.
- Conduct regular contract audits to identify fraudulent or erroneous data; for example, contractor overcharges, duplicate charges or excessive time logging. Don’t wait for a “gut feeling” to guide a decision to look at the numbers more closely.

Key questions and next steps
Organizations should ask key questions with respect to their contract risk and compliance posture
- Does our organization fully understand the meaning of Contract Risk and Compliance?
- Do we have a clear view of third-party relationships and related information across our entire business model?
- Have we identified key risks and risk management priorities for each?
- What communication structures and processes are in place with our vendors to eliminate assumptions and misunderstandings?
- Are we looking for opportunities to maximize the value of our business partnerships through contract management?
- Do we regularly review our contracts to ensure we’re receiving value on both costs incurred and services received?
- Have we taken steps to ensure that, when we become comfortable in a third-party relationship, we don’t slip back into any bad habits?
A contract is a guideline, not a guarantee

You cannot proceed with a business relationship simply assuming that a contract will be executed exactly as it is written. A contract is a guideline, within which both parties are accountable for performance – and assumed risk is rarely one-sided. Business relationships should be, and generally are, built on trust; don’t be afraid to verify the facts on which you base that trust. In the end, that verification increases the strength of your relationship. The best way to ensure all parties are adhering to the contract throughout its term is to establish regular communications right from the start, working through any misunderstandings or issues before they become major problems. Companies miss many opportunities from a return-on-investment perspective by not having full transparency of their own contract situation. Finding these opportunities are the right and responsibility of all parties to a contract. Your partners won’t feel guilty about taking vigilant action to preserve contract integrity, and neither should you.
Poll results

Which best describes your company’s approach to establishing contracts?*

A  23%  We have a dedicated contract management office or team that coordinates contract initiation with stakeholders from across the company

B  43%  Individual business units lead contract initiation and coordinate with relevant stakeholders (e.g. legal, finance, IT)

C  26%  Individual business units and the legal department jointly coordinate contract initiation

D  8%    Other

E  0%    Don’t know

Which response best describes your company’s approach to annual vendor contract administration?*

A  29%  We establish key performance indicators (KPIs) and key compliance indicators (KCIs) that we monitor for contract performance and compliance reviews at least annually

B  22%  We establish KPIs and KCIs but do not review vendor performance or compliance at regular intervals

C  21%  We establish KPIs or KCIs but do not monitor vendors for performance or compliance

D  21%  Our company does not ordinarily establish KPIs or KCIs for our vendors

E  7%    Don’t know

* Percentages rounded.
A not insignificant amount of money typically slips through the cracks in the average contract between organizations and external partners because of billing errors. There are various opportunities to recover this cash in any organization, but some are unique to each industry. The chart may help you hone your thinking about where and how to identify cost recovery opportunities that are common in your industry. (This exercise could be largely circumvented by implementing and adhering to a robust governance program for third-party contracts.)

### All industries
- Vendor cost recovery
- Claim validation
- Warranty assurance
- Regulatory compliance
- Software asset management
- Service provider inspections
- Revenue assurance

### Financial services
- Payment processor inspections
- Asset/securitization/trustee services
- Royalty compliance reviews
- Revenue share agreements

### Real estate
- Tenant lease inspections
- Percentage rent validation inspections
- Construction cost reporting

### Consumer Business
- Franchise revenue inspections
- Debt compliance
- Advertising agency inspections

### Technology, media & telecommunications
- IP / License reviews
- Distribution inspections (price protection, compensation programs)

### Energy and resources
- Capital projects
- Environmental regulations
- Health and safety
- Royalties

### Public service
- Social & regulatory compliance
- Federal grant/program inspections
- Supplier quality / government pricing reviews

### Manufacturing
- Sales rebate inspections
- Supplier compliance
- Warranty claims inspections

### Health care & life sciences
- Royalty compliance inspections
- Cost or revenue sharing inspections
- Provider benefits reporting
Internal Audit
Adding value in a changing landscape

Sensors that scan the environment for any and all emerging threats

A recent Wall Street Journal article referred to audit committees as “the board’s fire department.” Given that description, Internal Audit (IA) would have to be considered the board’s smoke detectors: sensors that scan the environment for any and all emerging threats. Certainly IA is increasingly viewed as critical by stakeholders in management and on the audit committee. However, the different perspectives of these various stakeholders – particularly on risk and where IA can add value – means IA must manage a range of expanding and shifting expectations.

Adapting to this changing environment is a growing challenge for Internal Audit. For starters, annual audit plans that are set in stone and rigidly executed are relics of the past. The dynamic global economy – and the variety, quantity and fluidity of risks it engenders – requires an equally dynamic and flexible IA approach that responds to a variety of factors. In the rapidly changing high-tech sector, for example, quarterly plans are the new normal, replacing static annual roadmaps. And in the oil and gas sector, where swiftly declining prices are creating significant stakeholder uncertainty, IA groups are responding to a range of potential risks in areas such as asset impairment, fraud related to earnings pressures, liquidity and industry consolidation.

While operating in a much more volatile environment than before, the IA function must go beyond simply fulfilling its traditional assurance role. It is now expected to provide value in ways such as cost reduction and process efficiency.

IA’s proliferating role is made clear by numerous emerging trends, including

• Dynamic and flexible audit planning based on changing risks (e.g., oil price decline, foreign exchange fluctuations)
• Focus on delivering greater value and often “doing more with the same or less”
• Increased scrutiny of emerging risk areas
• Added focus on risks across the extended enterprise
• Heightened expectations of the audit committee
• Growing reliance on data analytics to improve quality, efficiency and value
• Rising use of data visualization techniques to drive greater insights and communicate a more compelling “story”

Senior executives who recognize and access the depth and breadth of expertise of Internal Audit to tackle their most strategic risk areas would serve their organization well.
For some, IA’s most important role is advising executives and management on special projects or requests. They expect IA personnel to be true subject matter experts, providing genuine insight on organization-wide risks rather than merely fulfilling a fixed reporting and assurance duty. For others, the best way to determine value is to look at IA success in responding in an advisory capacity to fraud issues, trading irregularities, supply chain problems and the like.

But everywhere IA operates, expectations are for it to apply best-in-class practices, point out macro trends and properly assess management performance. If it is really delivering in these areas, the quality, relevance and influence of its recommendations will be clear.

An example of the increased use of best-in-class practices by IA is the evolution of the use of data analytics, which is transforming IA perhaps more than any trend to date. Analytics techniques and tools allow IA to search vast amounts of data sets for patterns exposing risk areas that would have been like looking for needles in a haystack just half a decade ago. Resources can then be focused on looking for a root cause and providing insight for dealing with those emerging risk areas and issues. In short, applying analytics allows IA to examine the needle instead of figuring out if there’s one in the haystack in the first place. The net result is that IA can add value without adding significant resources.

Another example of the expansion of IA’s mandate is Predictive Project Analytics (PPA), which takes existing data to evaluate projects in terms of their probability of success. By comparing current situations with those that existed for successfully completed projects, IA is able to use PPA to identify the likelihood of failure and highlight gaps that need to be addressed.

Rapid advances in information technology are also affecting how IA performs its role. As organizations continue to adopt new technologies to create and sustain a competitive advantage, they also continue to change the IT risk landscape. To meet these challenges, Internal Audit is slowly adapting its approach to Information Technology Internal Audit (IT IA), which focuses efforts on providing value through understanding and mitigating organizational IT risks rather than through traditional compliance audits.

This shift in role is demonstrated in the new focus areas many organizations are setting for Internal Audit. While compliance-focused audits certainly need to be performed, leading-practice companies are balancing these low-risk, low-value activities with audits that drive value into the organization and help diminish risks arising from emerging IT risk areas such as cognitive computing, open-source solutions and sensor proliferation.
Enhancing the value of IA is critical, but it does create the potential for conflict between providing assurance and giving advice. IA shouldn’t be doing the work of management. It should be a centre of expertise to evaluate risk exposures and to help management identify and weigh potential options, but business units must own the risks.

Striking the right balance is key. Independent assurance remains a core IA accountability that still must be effectively delivered. But most organizations will—or should — also seek IA advice on big issues. In a retail company with declining profits, for example, IA could assess best practices around innovation or product development to help the company be more competitive. And since those types of requests require resource allocation, it is important to prepare and have a specific plan that accounts for IA involvement beyond assurance.

Acknowledging assurance and advisory as relative function requirements, with the split appropriate to the specific company and stakeholder expectations, is the new normal. This not only derives maximum value from IA, but also keeps its staff vibrant, engaged and well-equipped to deliver their best work.
Dynamic role needs the right people

Answering to multiple stakeholders requires IA to understand and manage expectations. Clarity and strong communication are essential for knowing exactly what each stakeholder expects. And rather than just follow a pre-set plan, IA needs to constantly re-evaluate and adapt to remain relevant and useful to the organization beyond assurance — and that it’s viewed as such. Given their growing advisory capacity, passion and confidence are really table stakes for IA professionals. Effective IA leaders also need strong interactive skills, a willingness to listen and the ability to think on their feet. With the right people who can earn trust and respect, both inside and outside the function, IA should be able to adapt to its changing, challenging mandate and deliver both the essential assurance and added value stakeholders expect.

High-impact focus areas

The role of Internal Audit is expanding. Compliance-focused activities are still fundamental, but to add real value, IA needs to focus efforts on the business-critical areas that can help the organization gain a competitive advantage in the marketplace. These key areas are:

1. Predictive project analytics: uses advanced analytics to evaluate the likelihood of project success by identifying project strengths and key control gaps, enabling IA to advise management about options.

2. Advanced digital visualization: helps auditors discover meaningful patterns in vast amounts of data, allowing IA to provide deep analytical insights and practical information.

3. Continuous auditing: continual extraction of key data from business processes enables broader and more proactive reviews, resulting in a dynamic and flexible audit plan that can adapt more quickly to changing risks.

4. Cybercrime: IA should take a leading role in ensuring there’s a systematic approach in place to evaluate and strengthen the effectiveness of cyber risk management, and that the appropriate cybersecurity capabilities are in place.

5. Software asset management: operational reviews of software licensing compliance provide insightful analysis about gaps in processes and recommendations to address them; over the long term, these reviews could result in significant cost savings and reduce resources spent on vendor audits.

6. Vendor governance: vendor audits assess third-party risk and can have a positive financial impact through cost recovery and improved controls to prevent excessive costs in future; the use of advanced analytical tools and techniques can create unique insights into supply chain inefficiencies.

7. Fraud risk management: IA should either support management in implementing a risk-management framework (e.g., facilitating workshops) or in providing assurance over key elements in the framework (e.g., design and implementation of testing of key controls).

8. Risk and control culture: IA should develop (and execute) a framework to assess whether the existing risk and control culture and related processes, actions and “tone at the top” align with their organization’s values, ethics, risk strategy, appetite and approach.

9. Mergers and acquisitions: due to its vantage point and deep competencies related to governance, risk and compliance, IA is ideally positioned to play a key role in these high-risk activities before, during and after the transaction, from risk evaluation to due diligence procedures to the capture of synergy benefits.
One step at a time

Mitigating risk in today’s increasingly complex business world can be a painstaking responsibility. But, like any other major effort, the way forward is one step at a time.

If leaders could take only one step in each of the four critical areas explored here, which would have the most impact? For information technology, it might be to appoint a “chief risk officer” of sorts, someone removed from the fray of daily operations to assess the organization-wide picture, identify problem areas and find solutions. In cybersecurity, it could be to align cyber risk with business operations, so that investments and resources are focused on what really matters.

For contract compliance, keep asking periodic questions about the organization’s risk exposure in, and governance of, its third-party relationships: out of sight does not mean out of responsibility. Internal audit leaders might move to ensure they’re strategically oriented within the business such that Internal Audit is recognized as a valuable advisor.

Ultimately, risk considerations will always be in play because standing still is not an option. Making smart decisions while adopting new technologies and best practices to help you operate more efficiently and offer your customers new or improved products and/or services is the most intelligent way both to stay safe and maintain a competitive edge.

Indeed, striking a balance between effective risk mitigation and intelligent risk-taking is a complex, but not impossible, mission. It’s also necessary for a healthy, prosperous future. After all, everyone wants to enjoy the benefits that progress promises – provided missteps can be avoided. Being well-prepared reduces those chances considerably.
Risk series

Know the worth of risk

The Deloitte Risk Series is an annual exploration of the latest challenges in risk management. Join upcoming seminars to hear the perspectives of Deloitte risk professionals on the current environment and discover strategies for turning risk into value for your organization.

Terry Hatherell
Governance, Regulatory & Risk Leader
+1 416 643 8434
thatherell@deloitte.ca

Nick Galletto
Cyber Risk Services Leader
+1 416 601 6734
ngalletto@deloitte.ca

Andrew Kwong
Controls Transformation & Assurance Leader
+1 416 202 2784
akwong@deloitte.ca

www.deloitte.ca

Deloitte, one of Canada’s leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

© 2015 Deloitte LLP and affiliated entities.
Designed and produced by the Deloitte Design Studio, Canada. 15-3043T