Deloitte.

The Risk Intelligent IT internal auditor

IT IA takes flight

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.

Feeling bogged down?

Ever feel like your IT internal audit group just can't get off the ground? What's holding it down?

Auditors know there's truth in numbers, so here's a quick calculation sheet for you:

- How many boxes will your IT IA team check this year?
- How many general computer controls will they audit?
- How many years have you been telling management that it needs a comprehensive business continuity plan?
- How many years have they ignored that recommendation?

Here's the mundane truth for many organizations: IT IA has audited Unix for the last five years; IT IA is auditing Unix again this year. Nothing has changed.

If that describes your group, well, it's time to get out of the ditch. To retain relevance, IT IA must break free of its historical binds. It's not just about computer systems. (It never really was, but that's a topic for another conversation.) It's about understanding broader business issues. It's about forging connections between these issues and the technology that can help address them. It's about taking a Risk Intelligent approach that not only seeks to mitigate risks to existing assets but also encourages appropriate, calculated risk taking for reward.

Do these things well and your IT IA fleet will soon get unstuck.

High-flying IT IA

Which prototype best describes your IT internal audit group?

Type 1 — Drifting along: IT IA floats through its audit plan, engaged in traditional GCC and systems work, diligently checking the boxes, but with no clear destination in sight.

Type 2 — Getting aloft: IT IA has a little lift under its wings. The group helps drive current initiatives, such as M&A assessment and integration, system implementations, and IT risk assessment.

Type 3 — Flying high: IT IA soars with a clear view of the future. The group is involved in value-generating work, applying the principles of Risk Intelligence to both risks and opportunities. With its sophisticated radar, IT IA is addressing IT risks before they become issues.

The activities that fall under these types are, of course, cumulative. That is, IT IA groups in type 3 will also engage in all the activities of types 1 and 2, addressing both the day-to-day and the longer-term issues.

Where does your IT group fall along the continuum? More important — where do you want to be? The decision is entirely yours. Each type carries a different level of cost and provides a different level of value to your organization.

Type 1: Drifting along

Time to harness the winds of change?

Hot air balloons are wonderful for sightseeing, but not as useful if you have a particular destination and a specific arrival time in mind.

Perhaps your IT IA group favors a slow, meandering approach — executing the same audit plan year after year, coming up with similar findings audit after audit.

That may be fine for some companies. It may be aligned with your ambitions. It may be suitable for your team. And if that's the case, feel free to close this book. It's not for you.

But if you want to get someplace fast, if you wish to travel efficiently, and if you hope to move ahead of the pack, well, you'll need more than hot air to get you there. Consider this book your travel guide.

Is your IT IA organization "type 1" by choice or by default?

Type 2: Getting aloft

Before taxiing down the runway, make sure your IT IA group is airworthy. Here are some issues you should consider addressing.

New products and service lines

Your company has plenty going on. Mergers, acquisitions, and divestitures. New products. Expanded markets.

And your IT IA group may be pretty busy too. Unfortunately, it's probably "busy" as in "busy work," rather than meaningful, strategic work.

IT IA is typically not invited to join in the fun stuff: new product rollouts and new business streams. And that's a wasteful underutilization of IT IA's talents. The group can and should tackle a much broader set of business issues that generate revenue, not just addressing tasks intended to save money.

How can IT IA add value? Consider the example of the latest toy craze: web-linked, "huggable plush pets." The technology risks related to these playthings are considerable: Child privacy. Server demand. Data center impacts. To address these, IT IA should be at the forefront, consulted at every stage of the game, conducting pre- and post-implementation reviews.

Cut IT IA out of the picture, and you could be rolling out nothing more than, well, a stuffed animal.

Is your IT IA group involved in strategic initiatives?

M&A

Does "buyer's remorse" ever come into play during M&A? It's less likely if IT internal audit is involved.

Unlike any other group, IT IA understands the inherent — and often substantial — risks in attempting to integrate technology environments and controls. Not just the machinery, but the people who run it and the processes they use. And, really, isn't systems integration risk something you'd want on the table during the negotiation sessions, rather than after the deal is signed?

What effect would it have on deal valuation if IT IA was called on to assess the IT environment and controls integration risks?

In some cases, maybe deal valuation is not even the proper measure. How about deal viability?

At what stage of the M&A process is IT IA consulted? (Is it consulted at all?)

Contract Risk & Compliance

It's 2 a.m.

Do you know where your royalties are?

(Not to mention your rebates, commissions, incentives, and warranty payouts.)

In the modern enterprise, payments sent and received are funneled through IT. Controls around these processes need to be evaluated and managed. Who is doing this right now?

Stopping leakage is the goal. And IT IA should be the virtual plumbers. Sophisticated data analysis routines can be built by IT internal audit as part of a contract risk and compliance program.

If you are concerned that IT IA is perceived as a cost center rather than a revenue generator, then tackle CRC. Big money could be at stake.

Think of it as IT IA's recoup de grâce.

Is contract risk & compliance on this year's risk assessment?

Globalization

Globalization equals opportunity: New markets. Cheaper labor. Shortened supply chains. Abundant raw materials.

But what about the risks? A Risk Intelligent approach considers the risks that could prevent you from achieving your growth objectives.

Let's say your company wants to open a factory in a developing country. The project is past the point of no return when you are surprised to learn there is no fiber optic and limited copper wiring. Thus, communications between the home office and the outpost must be conducted through microwave, radio, or satellite. Naturally, major security issues accompany these modes.

IT IA could have alerted management to these issues during the decision-making process. As the (globalized) saying goes, a gram of prevention is worth a kilo of cure.

But IT infrastructure issues barely scratch the surface. What about the physical security of your new Third World data center? What about transportation issues? How easy will it be to bring in a service team to deal with an IT issue? How about availability and access to qualified people? What about local regulations regarding privacy and data movement?

Plenty of issues for IT IA to tackle. Remember: It's never too late to save management from itself.

Is IT IA consulted on foreign expansion plans?

The regulatory present

How deep has IT IA waded into the regulatory thicket? Probably not deep enough. SOX is pretty well beaten back, but what about HIPAA, the Safe Harbor Act, and other privacy related regs? In these areas, oversight often sits in the legal department. But let's be real — are they up to the task? Lawyers often have no training or experience in IT risks and controls.

Many leading companies are exploring ways to bring efficiencies to regulatory compliance. After all, many of the recordkeeping and documentation requirements are similar, many of the same people are responsible for multiple regs, and many of the processes would lend themselves to consolidation. Sounds like a perfect opportunity for IT IA to get involved, doesn't it?

Of course, a Risk Intelligent IT IA group doesn't limit itself to present-day concerns; it is always casting an eye to the future. And on the horizon lurk big issues.

Is the full spectrum of regulatory compliance on this year's risk assessment?

Type 3: Flying high

Break free of the gravitational pull that holds back IT IA. Here are some preflight issues to address.

The regulatory future

What are these big regulatory issues? Well, if the past offers any guidance, there will be plenty.

Two of particular concern loom just ahead, one regarding financial reporting — IFRS — and another involving nonfinancial reporting — climate change.

Has your IT IA group thought about the challenges posed by global financial reporting? How many entities will need to be converted? What is the process? How much will it cost?

Has the IT IA team considered carbon emission reporting? Cap and trade schemes? Carbon tax?

These issues will place a huge burden on IT IA shops. And make no mistake, they are arriving; the only question is how soon. IT IA groups that are happily oblivious to the threats will be deemed irrelevant.

Meanwhile, Risk Intelligent IT IA groups will work to shape the future, instead of being victimized by it.

Does IT IA help the company anticipate and prepare for upcoming regulations?

Green IT

When it comes to the G word, IT is clearly part of the problem. Your IT systems:

- Suck up huge amounts of energy
- Throw off large amounts of heat
- Cast off significant quantities of hazardous waste (such as heavy metals in obsolete computer monitors).

Without a doubt, you've got to clean your own house first.

But IT IA can also help drive a bigger solution. The group can:

- Help make sure the company anticipates and prepares for compliance with environmental regulations
- Help gain a return on the "going green" investment by consulting on power consumption, waste disposal, green purchasing, paper usage, and water usage
- Design data collection systems for energy use, carbon emissions, recycling rates, water usage, and other "footprint" issues.

Your company is accustomed to — and presumably good at — gathering data for financial reporting. But nonfinancial measures represent less familiar terrain. It may be up to IT IA to blaze the path to this green future.

Have you conducted a green IT audit?

Is it on this year's risk assessment?

Emerging reporting standards

IFRS is inevitable. Depending on the size and complexity of your organization, it may provoke a pebble-like ripple or it may wash over you like a tsunami. IFRS will require significant changes in application configurations within your organization.

XBRL may not be far behind. Although the prospect of a regulatory mandate is not as certain, Risk Intelligent organizations will prepare as if it were.

Remember the frenzy around SOX? In this case, you've got a longer runway. Smart IT IA shops will use the lead time to help their organizations understand the issues and risks, to help drive decision-making, and to help determine the migration path and timing of the change-overs.

Have you done a readiness assessment of your systems' ability to adapt to evolving reporting requirements?

Is it on this year's risk assessment?

Continuous controls monitoring

What's a surefire way to gain management approval for an IT IA-initiated project? Propose something that makes their job easier.

CCM is commonly thought to mainly benefit internal audit, but that's a misconception. Continuous controls monitoring tools can give management fresher, cleaner, better information. And improved data yields improved decision making. (Like the decision, say, to give you a raise.)

CCM can also help reduce the amount of testing performed by external auditors. (Less money to auditors; more money for that raise.)

Internal control is uppermost in management's mind. Yet C-suite attention spans are notoriously short. IT IA is in a prime position to help socialize, educate, demonstrate, and help implement CCM. Act expeditiously.

Have you evaluated the opportunities to automate controls monitoring and determined what ROI could be achieved?

Industrial espionage, computer piracy and technology terrorism

As critical assets become digitized, they become easier to steal. Product design specs. Patent applications. Music and film. Strategic plans and intelligence. Confidential communications. Upon conversion to ones and zeros, vulnerability increases.

How sturdy are your lines of defense? IT IA has the means to find out.

But when you deploy the troops, think broadly about your theater of operations. Consider not just a single category of intellectual property, but rather, the vulnerability of your entire IT infrastructure. Could a black hat attack cripple your company?

A debilitating cyber-attack is not some far-fetched fantasy. For example, in the spring of 2007, the Baltic country of Estonia endured a massive three-week assault that disabled the websites of businesses, government offices, media, and banks. The country was essentially shut down by a well-coordinated group of hackers.

Technology terrorism may be the next business battleground. Is your IT IA shop ready to defend the homeland?

Have you performed a digital asset assessment and risk ranking?

Have you evaluated your lines of defense against espionage, piracy, and terrorism?

Embedded processing units

Kiosks have become as ubiquitous as the phone booths of yesteryear. Supermarket self-checkout stations. Airport ticketing machines. Standalone ATMs.

EPUs have smart manufacturing and programming logic built in, along with autonomous functions, operating system, and software. Like HAL of "2001," they almost qualify as independent life forms. And like that rogue computer, they can cause problems if not properly managed. For example …

- How do you update the OS and software?
- How do you secure the units?
- Do you know what networks they are attached to?
- How do you know if they are compromised?
- What safeguards are in place?
- Or maybe the question is more basic: Do you even have an accurate inventory of EPU installs?

Have you determined what embedded systems are in place or planned?

Have you evaluated the risk around these?

Foreign Corrupt Practices Act and Office of Foreign Assets Control

What acronyms keep executives awake at night? Along with SOX, you can include FCPA and OFAC. Perhaps it's the legal requirements. Or the hefty fines. The tarnished reputation. Or the prospect of relocating to federal digs. Whatever the source of insomnia, IT IA can offer a soporific.

Compliance with these and other requirements can be automated and system driven. IT IA should work with legal counsel to help provide a solution that is effective and efficient.

Example: Consider an automated process that compares current and proposed vendors and customers against the OFAC list. IT IA can help follow up on identified issues.

Have you evaluated FCPA and OFAC compliance processes?

Have you rationalized solutions?

Is this issue on your risk assessment?

The Risk Intelligent IT internal auditor

What do you want your IT IA group to be when it grows up? Drifting along and just getting by? Or flying high and helping propel success?

IT IA brings unique aptitude and perspective to the organization. But in many companies, these talents are woefully underutilized.

A proactive approach can help elevate the group. A Risk Intelligent IT IA group doesn't wait around for something to get done so they can audit it. Rather, the group conducts a Risk Intelligent IT risk assessment that addresses not just protection of existing assets but also strategic risk taking for reward.

IT IA jostles, cajoles, and inserts itself into key initiatives. It peers into the future. It outlines the uncomfortable scenarios. It asks the prodding questions. And it provides the wise counsel and technological know-how to keep the company's trajectory rising.

It's time for takeoff. T minus zero approaches.

Have you made a deliberate strategic decision on the optimal profile and activities of IT internal audit?

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.